CHAPTER 6

# INTELLECTUAL PROPERTY

## QUOTE

*Intellectual property has the shelf life of a banana.*
—Bill Gates, founder of Microsoft

## VIGNETTE

### Sinovel Steals Millions in Trade Secrets from American Superconductor

In 2006, the Chinese government passed a clean air energy law that mandated the creation of seven giant wind farms, each of which would, within a decade and a half, produce as much energy as 10 nuclear reactors. Daniel McGahn, vice president in charge of new business for American Superconductor (AMSC), saw a tremendous opportunity for his company in China. Over the course of the next several years, AMSC made deals with several Chinese companies that would manufacture wind turbines for which AMSC would supply the electronic control systems, the software, and the electrical components necessary to transform the wind energy generated into electrical power.[1] And for a while, that strategy paid off.

AMSC produces advanced smart grid technology for power companies and electronic control systems that maximize wind turbine reliability, availability, and energy output. Yet American power companies have been reluctant to update their systems with smart grid technology that could prevent outages simply because of the huge cost involved in such an investment.[2] So, the Chinese

wind legislation was a windfall for AMSC. AMSC stock quadrupled in value between 2006 and 2009.[3]

AMSC's largest customer in China was Sinovel Wind Group, a company that had bid on and won 47 percent of the Chinese government's wind projects. Sinovel captured a leading position in China's wind market. However, as more and more Chinese companies began producing turbines, the price of turbines dropped by 40 percent, and Sinovel's profits also dropped. Still, AMSC had multiyear contracts with Sinovel at set prices, and Sinovel continued to produce large quantities of turbines equipped with AMSC technology.



In March 2011, Sinovel began rejecting AMSC shipments of electronic components—shipments worth more than $70 million—without explanation. In April of that year, AMSC was forced to announce that Sinovel had stopped placing orders, despite the fact that AMSC had contracts committing Sinovel to $700 million in future orders. Daniel McGahn, now CEO of AMSC, tried to uncover the problem and mend relations, but Sinovel declined to resume placing orders. Then, in June 2011, a group of AMSC engineers testing a Sinovel turbine in northern China uncovered electrical components that were running a stolen version of AMSC software. Sinovel had somehow accessed AMSC proprietary source code and was manufacturing its own electrical components, cutting AMSC out of the operation.[4]

In 2010 and 2011, China had experienced major disruptions in its power grids as disturbances, such as trees falling on lines, shut down thousands of turbines. The Chinese government proposed legislation to require energy companies such as Sinovel to upgrade their electrical components with software that would allow wind farms to continue to function despite power grid disturbances. Because AMSC software controlled all of Sinovel's existing turbines, Sinovel would be required to

purchase the software upgrade from AMSC.[5] Instead, Sinovel recruited an Austrian-based AMSC engineer, Dejan Karabasevic, to develop the necessary software. Sinovel signed an employment contract with Karabasevic and flew him to an apartment in Beijing, along with code stolen from AMSC's servers in Austria. He then spent several weeks reverse engineering the software to come up with the source code necessary to install in Sinovel's turbines.



After AMSC discovered the stolen software, the company was able to track it back to Karabasevic. Ultimately, Karabasevic confessed to Austrian police and was sentenced to 12 months in prison for revealing trade secrets.[6] AMSC filed several lawsuits against Sinovel in Chinese courts, seeking $1.2 billion in damages for intellectual property theft and breach of contract, while Sinovel has countersued for $207 million, claiming AMSC provided substandard quality equipment. The court battle, which garnered the attention of top U.S. and Chinese officials, is seen as a test case. Many Western companies (including DuPont, Google, and Lockheed Martin) have claimed that they have been victims of Chinese espionage, and the court's decision will be an indication of whether China is willing to restrict such behavior.[7] China's Supreme Court surprised many when it agreed to review lower court decisions dismissing one of AMSC's claims.[8]

The director of the National Security Agency has called the theft of technological secrets by Chinese companies from U.S. and Western companies "the greatest transfer of wealth in history."[9] American leaders perceive these cases not as isolated incidents, but rather as part of a larger strategy of employing unfair trading practices—similar to China's decision to corner the market on rare earth metals needed to produce high-tech hardware. The U.S. International Trade Commission has estimated that if China instituted intellectual property protection measures similar to those in the United States, the United States would gain between 900,000 and 2.1 million jobs.[10] Yet AMSC and many other Western companies continue to do business in China.

AMSC is still working to recover from its 2011 losses when its stock dropped from almost $30 to $4 per share. The company has signed deals in Korea, India, and Russia for its electrical control systems, and Daniel McGahn recently noted that "silver linings are beginning to appear" as China is forecasting an increase in wind turbine installations now that stricter quality regulations have been implemented.[11]



### Questions to Consider

1. What additional evidence would convince you that China's theft of technological secrets represents a national strategy rather than just a series of isolated incidents?
2. What actions might Western countries take to protect the loss of technological secrets and to reduce the risk of continuing to do business in China?

### LEARNING OBJECTIVES

**As you read this chapter, consider the following questions:**

1. What does the term *intellectual property* encompass, and why are organizations so concerned about protecting intellectual property?
2. What are the strengths and limitations of using copyrights, patents, and trade secret laws to protect intellectual property?
3. What is plagiarism, and what can be done to combat it?
4. What is reverse engineering, and what issues are associated with applying it to create a lookalike of a competitor's software program?
5. What is open source code, and what is the fundamental premise behind its use?
6. What is the essential difference between competitive intelligence and industrial espionage, and how is competitive intelligence gathered?
7. What is cybersquatting, and what strategy should be used to protect an organization from it?

## WHAT IS INTELLECTUAL PROPERTY?

**Intellectual property** is a term used to describe works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct and owned or created by a single person or group. Intellectual property is protected through copyright, patent, and trade secret laws.

Copyright law protects authored works, such as art, books, film, and music; patent law protects inventions; and trade secret law helps safeguard information that is critical to an organization's success. Together, copyright, patent, and trade secret legislation form a complex body of law that addresses the ownership of intellectual property. Such laws can also

present potential ethical problems for IT companies and users—for example, some innovators believe that copyrights, patents, and trade secrets stifle creativity by making it harder to build on the ideas of others. Meanwhile, the owners of intellectual property want to control and receive compensation for the use of their intellectual property. Should the need for ongoing innovation or the rights of property owners govern how intellectual property is used?

Defining and controlling the appropriate level of access to intellectual property are complex tasks. For example, protecting computer software has proven to be difficult because it has not been well categorized under the law. Software has sometimes been treated as the expression of an idea, which can be protected under copyright law. In other cases, software has been treated as a process for changing a computer's internal structure, making it eligible for protection under patent law. At one time, software was even judged to be a series of mental steps, making it inappropriate for ownership and ineligible for any form of protection.



## COPYRIGHTS

Copyright and patent protection was established through the U.S. Constitution, Article I, section 8, clause 8, which specifies that Congress shall have the power "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Rights to their respective Writings and Discoveries."

A **copyright** is the exclusive right to distribute, display, perform, or reproduce an original work in copies or to prepare derivative works based on the work. Copyright protection is granted to the creators of "original works of authorship in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."[12] The author may grant this exclusive right to others. As new forms of expression develop, they can be awarded copyright protection. For example, in the Copyright Act of 1976, audiovisual works were given protection, and computer programs were assigned to the literary works category.

**Copyright infringement** is a violation of the rights secured by the owner of a copyright. Infringement occurs when someone copies a substantial and material part of another's copyrighted work without permission. The courts have a wide range of discretion in awarding damages—from $200 for innocent infringement to $100,000 for willful infringement.

### Copyright Term

Copyright law guarantees developers the rights to their works for a certain amount of time. Since 1960, the term of copyright has been extended 11 times from its original limit of 28 years. The Copyright Term Extension Act, also known as the Sonny Bono Copyright Term Extension Act (after the legislator, and former singer/entertainer, who was one of the cosponsors of the bill in the House of Representatives), signed into law in 1998, established the following time limits:

- For works created after January 1, 1978, copyright protection endures for the life of the author plus 70 years.
- For works created but not published or registered before January 1, 1978, the term endures for the life of the author plus 70 years, but in no case expires earlier than December 31, 2004.

- For works created before 1978 that are still in their original or renewable term of copyright, the total term was extended to 95 years from the date the copyright was originally secured.[13]

These extensions were primarily championed by movie studios concerned about retaining rights to their early films. Opponents argued that lengthening the copyright period made it more difficult for artists to build on the work of others, thus stifling creativity and innovation. The Sonny Bono Copyright Term Extension Act was legally challenged by Eric Eldred, a bibliophile who wanted to put digitized editions of old books online. The *Eldred v. Ashcroft* case went all the way to the Supreme Court, which ruled the act constitutional in 2003.[14]



## Eligible Works

The types of work that can be copyrighted include architecture, art, audiovisual works, choreography, drama, graphics, literature, motion pictures, music, pantomimes, pictures, sculptures, sound recordings, and other intellectual works, as described in Title 17 of the U.S. Code. To be eligible for a copyright, a work must fall within one of the preceding categories, and it must be original. Copyright law has proven to be extremely flexible in covering new technologies; thus, software, video games, multimedia works, and Web pages can all be protected. However, evaluating the originality of a work is not always a straightforward process, and disagreements over whether or not a work is original sometimes lead to litigation. For example, former Beatles member George Harrison was entangled for decades in litigation over similarities between his hit "My Sweet Lord," released in 1970, and "He's So Fine," composed by Ronald Mack and recorded by the Chiffons in 1962.[15]

Some works are not eligible for copyright protection, including those that have not been fixed in a tangible form of expression (such as an improvisational speech) and those that consist entirely of common information that contains no original authorship, such as a chart showing conversions between European and American units of measure.

## Fair Use Doctrine

Copyright law tries to strike a balance between protecting an author's rights and enabling public access to copyrighted works. The **fair use doctrine** was developed over the years as courts worked to maintain that balance. The fair use doctrine allows portions of copyrighted materials to be used without permission under certain circumstances. Title 17, section 107, of the U.S. Code established that courts should consider the following four factors when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty:

- The purpose and character of the use (such as commercial use or nonprofit, educational purposes)
- The nature of the copyrighted work
- The portion of the copyrighted work used in relation to the work as a whole
- The effect of the use on the value of the copyrighted work[16]

The concept that an idea cannot be copyrighted but the expression of an idea can be is key to understanding copyright protection. For example, an author cannot copy the

exact words that someone else used to describe his feelings during a skirmish with terrorists, but he can convey the sense of horror that the other person expressed. Also, there is no copyright infringement if two parties independently develop a similar or even identical work. For example, if two writers happened to use the same phrase to describe a key historical figure, neither would be guilty of infringement. Of course, independent creation can be extremely difficult to prove or disprove.

The HathiTrust Digital Library is a joint project involving major research institutions, the libraries of several universities, and Google. The intent of the project was for Google to create a searchable database of the holdings of the participants, along with tools to facilitate access and searching of the database.[17] However, in 2011, the Authors Guild, an advocacy group for writers, filed a lawsuit alleging the project violated copyright law because the process of creating and accessing the digital library involved the unauthorized creation of multiple copies of the books. HathiTrust argued that its use of the material was "transformative" and thus permissible under conditions of the fair use doctrine. In this situation, a transformative act is one in which enough new material is added to a work to change the nature of the work or to modify the purpose for which the work is intended. The judge in the case reasoned that scanning and indexing the books for the purpose of allowing readers to search the content was indeed transformative and ruled in favor of HathiTrust.[18,19]



## Software Copyright Protection

The use of copyrights to protect computer software raises many complicated issues of interpretation. For example, a software manufacturer can observe the operation of a competitor's copyrighted program and then create a program that accomplishes the same result and performs in the same manner. To prove infringement, the copyright holder must show a striking resemblance between its software and the new software that could be explained only by copying. However, if the new software's manufacturer can establish that it developed the program on its own, without any knowledge of the existing program, there is no infringement. For example, two software manufacturers could conceivably develop separate but nearly identical programs for a simple game such as tic-tac-toe without infringing the other's copyright.

Tetris is a very popular computer game that was created in 1984. Over the years, versions of Tetris have been developed and licensed to run on Nintendo's Game Boy, DS, and Wii; Sony's PlayStation; Apple's iPod, iTouch, and iPhone; and Android phones.[20] Xio Interactive was a small company formed for the purpose of creating an unlicensed iPhone version of Tetris—named Mino.[21] However, shortly after Xio posted its Mino app to the Apple iTunes store, Tetris filed a copyright infringement lawsuit against the company. In its defense, Xio argued that because it only copied the rules and basic functionality of the game, and not its more original components, there was no infringement. While the court agreed that the fundamental rules and basic functionality of the game could not be protected, it pointed out that many other elements of the game had been copied, including the color, shape, and number of game bricks; how the pieces were formed from the game bricks; and the manner in which the pieces moved. In addition, the court noted that screen shots of the games viewed side by side were nearly

identical. The court ruled that Xio was permanently banned from selling, displaying, or promoting the Mino game.[22]

## The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008

The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 increased trademark and copyright enforcement and substantially increased penalties for infringement. For example, the penalty for infringement of a 10-song album was raised from $7,500 to $1.5 million. The law also created the Office of the United States Intellectual Property Enforcement Representative within the U.S. Department of Justice. One of its programs, called CIIIP (Computer Hacking and Intellectual Property), is a network of over 150 experienced and specially trained federal prosecutors who focus on computer and intellectual property crimes.[23]



## General Agreement on Tariffs and Trade (GATT)

The General Agreement on Tariffs and Trade (GATT) was a multilateral agreement governing international trade. There were several rounds of negotiations addressing various trade issues. The Uruguay Round, completed in December 1993, resulted in a trade agreement among 117 countries. This agreement also created the World Trade Organization (WTO) in Geneva, Switzerland, to enforce compliance with the agreement. GATT includes a section covering copyrights called the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), discussed in the following section. U.S. intellectual property law was amended to be essentially consistent with GATT through both the Uruguay Round Agreements Act of 1994 and the Sonny Bono Copyright Term Extension Act of 1998. Despite GATT, however, copyright protection varies greatly from country to country, and an expert should be consulted when considering international usage of any intellectual property.

## The WTO and the WTO TRIPS Agreement (1994)

The World Trade Organization (WTO) is a global organization that deals with rules of international trade based on WTO agreements that are negotiated and signed by representatives of the world's trading nations. The WTO is headquartered in Geneva, Switzerland, and had 158 member nations as of February 2013. The goal of the WTO is to help producers of goods and services, exporters, and importers conduct their business.[24]

Many nations recognize that intellectual property has become increasingly important in world trade, yet the extent of protection and enforcement of intellectual property rights varies around the world. As a result, the WTO developed the **Agreement on Trade-Related Aspects of Intellectual Property Rights**, also known as the TRIPS Agreement, to establish minimum levels of protection that each government must provide to the intellectual property of all WTO members. This binding agreement requires member governments to ensure that intellectual property rights can be enforced under their laws and that penalties for infringement are tough enough to deter further violations. Table 6-1 provides a brief summary of copyright, patent, and trade secret protection under the TRIPS Agreement.

**TABLE 6-1** Summary of the WTO TRIPS Agreement

| Form of intellectual property | Key terms of agreement |
|---|---|
| Copyright | Computer programs are protected as literary works. Authors of computer programs and producers of sound recordings have the right to prohibit the commercial rental of their works to the public. |
| Patent | Patent protection is available for any invention—whether a product or process—in all fields of technology without discrimination, subject to the normal tests of novelty, inventiveness, and industrial applicability. It is also required that patents be available and patent rights enjoyable without discrimination as to the place of invention and whether products are imported or locally produced. |
| Trade secret | Trade secrets and other types of undisclosed information that have commercial value must be protected against breach of confidence and other acts that are contrary to honest commercial practices. However, reasonable steps must have been taken to keep the information secret. |

Source Line: World Trade Organization, "Overview: The TRIPS Agreement," www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

## The World Intellectual Property Organization (WIPO) Copyright Treaty (1996)

The World Intellectual Property Organization (WIPO), headquartered in Geneva, Switzerland, is an agency of the United Nations established in 1967. WIPO is dedicated to "the use of intellectual property as a means to stimulate innovation and creativity." It has 185 member nations and administers 25 international treaties. Since the 1990s, WIPO has strongly advocated for the interests of intellectual property owners. Its goal is to ensure that intellectual property laws are uniformly administered.[25]

The WIPO Copyright Treaty, adopted in 1996, provides additional copyright protections to address electronic media. The treaty ensures that computer programs are protected as literary works and that the arrangement and selection of material in databases is also protected. It provides authors with control over the rental and distribution of their work, and prohibits circumvention of any technical measures put in place to protect the works. The WIPO Copyright Treaty is implemented in U.S. law through the Digital Millennium Copyright Act (DMCA), which is discussed in the next section.

## The Digital Millennium Copyright Act (1998)

The **Digital Millennium Copyright Act** (DMCA) was signed into law in 1998 and implements two 1996 WIPO treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The act is divided into the following five sections:

- *Title I (WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998)*—This section implements the WIPO treaties by making certain technical amendments to U.S. law in order to provide appropriate references and links to the treaties. It also creates two new prohibitions in the Copyright Act (Title 17 of the U.S. Code)—one on

circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information. Title I also adds civil remedies and criminal penalties for violating the prohibitions.

- *Title II (Online Copyright Infringement Liability Limitation Act)*—This section enables Web site operators that allow users to post content on their Web site (e.g., music, video, and pictures) to avoid copyright infringement liability if certain "safe harbor" provisions are followed.
- *Title III (Computer Maintenance Competition Assurance Act)*—This section permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer. The new copy cannot be used in any other manner and must be destroyed immediately after the maintenance or repair is completed.
- *Title IV (Miscellaneous provisions)*—This section adds language to the Copyright Act confirming the Copyright Office's authority to continue to perform the policy and international functions that it has carried out for decades under its existing general authority.
- *Title V (Vessel Hull Design Protection Act)*—This section creates a new form of protection for the original design of vessel hulls.

The portion of Title I dealing with anticircumvention provisions makes it an offense to do any of the following:

- Circumvent a technical protection.
- Develop and provide tools that allow others to access a technologically protected work.
- Manufacture, import, provide, or traffic in tools that enable others to circumvent protection and copy a protected work.

Violations of these provisions carry both civil and criminal penalties, including up to five years in prison, a fine of up to $500,000 for each offense, or both. Unlike traditional copyright law, the DMCA does not govern copying; instead, it focuses on the distribution of tools and software that can be used for copyright infringement as well as for legitimate noninfringing use. Although the DMCA explicitly outlaws technologies that can defeat copyright protection devices, it does permit reverse engineering for encryption, interoperability, and computer security research.

Several cases brought under the DMCA have dealt with the use of software to enable the copying of DVD movies. For example, motion picture companies supported the development and worldwide licensing of the Content Scramble System (CSS), which enables a DVD player (shown in Figure 6-1) or a computer drive to decrypt, unscramble, and play back motion pictures on DVDs, but not copy them.

However, a software program called DeCSS can break the encryption code and enable users to copy DVDs. The posting of this software on the Web in January 2000 led to a lawsuit by major movie studios against its author. After a series of cases, courts finally ruled that the use of DeCSS violated the DMCA's anticircumvention provisions.

Title II provides "safe harbors" for ISPs whose customers/subscribers might be breaking copyright laws by downloading, posting, storing, or sending copyrighted material via its services. If an ISP has knowledge of infringing material and fails to take action to remove the

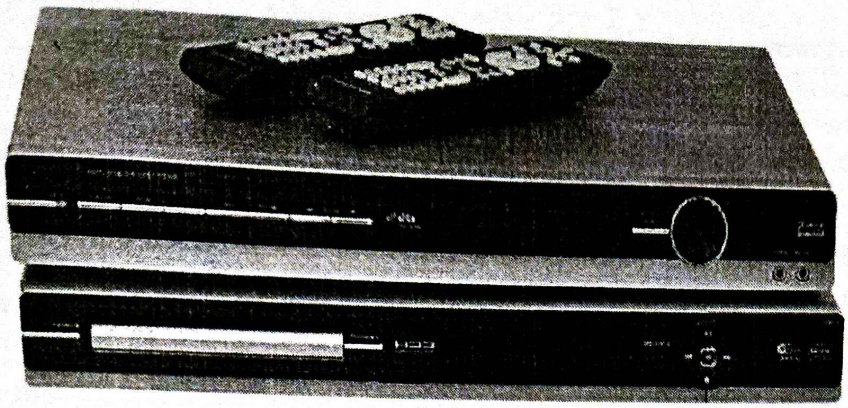

**FIGURE 6-1** Several cases brought under the DMCA have dealt with the use of software to enable the copying of DVD movies

Credit: © Polat/Shutterstock.com

material, it is not protected by the safe harbor measures. The ISP must also comply with clearly defined "notice and takedown" procedures that grant copyright holders a quick and simple way to halt access to allegedly infringing content. Copyright holders are granted the right to issue subpoenas to alleged copyright infringers identified through their ISP. Title II of the DMCA also provides defined procedures for ISP users to challenge improper takedowns.

The takedown procedure works as follows. The owners of copyrighted material who allege that their material has been infringed send a notice to the ISP hosting the content. The ISP forwards the notice to whoever was responsible for uploading material. That individual is given a chance to respond. If there is no response, the ISP must ensure that the material is no longer accessible. The ISP forfeits its protection under the safe harbor conditions if it fails to remove the material in a prompt manner.

Because many copyright infringers take measures to conceal their true identity, copyright owners must take additional steps if they wish to sue for copyright infringement. Provided a copyright owner has sent a DMCA notice, a John Doe subpoena can be obtained from a court clerk without even commencing a lawsuit. The subpoena compels the ISP to reveal the identity of the anonymous poster. The ISP is unlikely to resist the subpoena due to the associated legal costs.

The typical process for such lawsuits is that the IP addresses are collected for the alleged copyright violators. Attorneys then file a John Doe complaint in federal court and request the court to issue subpoenas to all ISPs used by the defendants. The subpoenas compel the ISPs to provide the defendants' names and other contact information. The attorneys then contact the defendants to offer them the opportunity to settle out of court and thus avoid embarrassment and legal fees.

Viacom International filed a $1 billion copyright infringement lawsuit against YouTube and its parent company Google in March 2007. Viacom alleged that YouTube violated the DMCA by permitting its users to post copyright-protected material from Viacom's various networks and subsidiaries—including Comedy Central, MTV, BET, and Paramount Pictures—without permission. Initially, a district court ruled that YouTube was immune from copyright liability because it was protected by the safe harbor provisions of the DMCA, even though Viacom had argued that YouTube had a "general awareness" of widespread infringement, which should disqualify YouTube from safe harbor protections.[26] Upon

appeal, the Second Circuit Court of Appeals determined that internal email exchanges among YouTube employees suggested that YouTube may have had specific knowledge of some infringing film clips. In April 2012, the Second Circuit Court of Appeals reinstated Viacom's lawsuit, and ordered the district court to reexamine the case to determine if YouTube is entitled to DMCA safe harbor protection.[27]

Some see the DMCA as a boon to the growth of the Internet and its use as a conduit for innovation and freedom of expression. Without the safe harbors that the DMCA provides, the risk of copyright liability would be so great as to seriously discourage ISPs from hosting and transmitting user-generated content. Others see the DMCA as extending too much power to copyright holders. They share the viewpoint of Verizon General Counsel William P. Barr, who stated in testimony before Congress that the "broad and promiscuous subpoena procedure" of the DMCA grants "truly breathtaking powers to anyone who can claim to be or represent a copyright owner; powers that Congress has not even bestowed on law enforcement and national security personnel."[28]



## PATENTS

A **patent** is a grant of a property right issued by the United States Patent and Trademark Office (USPTO) to an inventor. A patent permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators. Unlike a copyright, a patent prevents independent creation as well as copying. Even if someone else invents the same item independently and with no prior knowledge of the patent holder's invention, the second inventor is excluded from using the patented device without permission of the original patent holder. The rights of the patent are valid only in the United States and its territories and possessions. Figure 6-2 shows the number of patents applied for and granted in recent years.

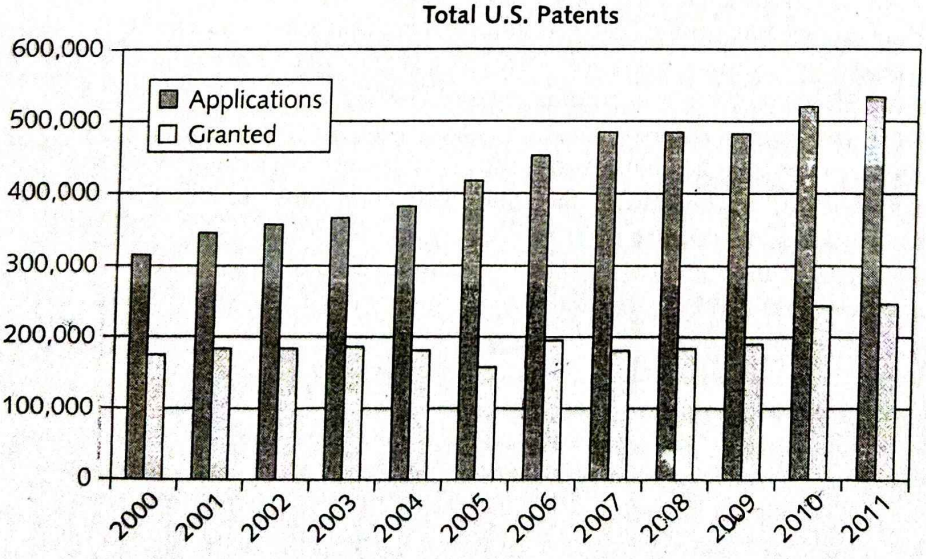


**FIGURE 6-2** Patents applied for and granted
Source Line: U.S. Patent Statistics Calendar Years 1963–2011, www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.pdf.

IBM obtained 6,478 patents in 2012, the 20th consecutive year it received more patents than any other company in the United States.[29] By some estimates, IBM's licensing of patents and technologies generates several hundred million dollars in annual revenue for the company.[30] Table 6-2 lists the IT organizations that were granted the most patents in 2012.

**TABLE 6-2** IT organizations that received the most patents in 2012

| Organization | Number of patents granted | Increase over 2011 |
|---|---|---|
| IBM | 6,478 | 5% |
| Samsung | 5,081 | 4% |
| Canon | 3,174 | 12% |
| Microsoft | 2,613 | 13%[31] |
| Google | 1,151 | 170% |
| Apple | 1,136 | 68% |

Source Line: "IBM Top Patent Producer 20 Years Running," *CNM Online*, January 13, 2013, www.cnmeonline.com/news/ibm-top-patent-producer-20-years-running.



To obtain a U.S. patent, an application must be filed with the USPTO according to strict requirements. As part of the application, the USPTO searches the **prior art**—the existing body of knowledge available to a person of ordinary skill in the art—starting with patents and published material that have already been issued in the same area. The USPTO will not issue a patent for an invention whose professed improvements are already present in the prior art. Although the USPTO employs 7,800 patent examiners to research the originality of each patent application, the average time from filing until the application is issued as a patent or abandoned by the applicant is around 31 months as of January 2013. At the end of 2012, there was a backlog of 597,579 unexamined patent applications.[32] Such delays in getting patents approved can be costly for companies that want to bring patented products to market quickly. As a result, in many cases, people trained in the patent process, rather than the inventors themselves, prepare patent applications.

The main body of law that governs patents is contained in Title 35 of the U.S. Code. Section 101 of the code states that "whoever invents or discovers any new or useful process, machine, manufacture or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor." Section 102 defines novelty as a necessary condition to grant a patent and describes various kinds of prior art which can be used as evidence that the invention is not novel. Section 103 describes "nonobviousness" as another mandatory requirement for a patent. To be patentable, an invention must not be obvious to a person having ordinary skill in the field on which the invention is based.

The U.S. Supreme Court has ruled that three classes of items cannot be patented: abstract ideas, laws of nature, and natural phenomena. Standing on its own, mathematical subject matter is also not entitled to patent protection. Thus, Pythagoras could not have patented his formula for the length of the hypotenuse of a right triangle ($c^2 = a^2 + b^2$). The statute does not identify computer software, gene sequences, or genetically modified bacteria as patentable subject matter. However, these items have subsequently been determined to be patentable.

Patent infringement, or the violation of the rights secured by the owner of a patent, occurs when someone makes unauthorized use of another's patent. Unlike copyright infringement, there is no specified limit to the monetary penalty if patent infringement is found. In fact, if a court determines that the infringement is intentional, it can award up to three times the amount of the damages claimed by the patent holder. The most common defense against patent infringement is a counterattack on the claim of infringement and the validity of the patent itself. Even if the patent is valid, the plaintiff must still prove that every element of a claim was infringed and that the infringement caused some sort of damage.



## Leahy-Smith America Invents Act (2011)

The **Leahy-Smith America Invents Act** represents a major change in U.S. patent law. Under this law, which was passed in 2011, the U.S. patent system changed from a "first-to-invent" to a "first-inventor-to-file" system effective March 16, 2013. That means if two people file for a patent application on the same invention at approximately the same time, the first person to file with the USPTO will receive the patent, not necessarily the person who actually invented the item first.[33,34]

The America Invents Act also expanded the definition of prior art used to determine the novelty of an invention and whether it can be patented. For example, if something resembling your invention were on sale anywhere in the world before you filed for a patent, that item is now considered part of the prior art and could prevent you from obtaining a patent. Prior to the passing of this law, only items for sale within the United States were considered prior art. The America Invents Act makes it more difficult to obtain a U.S. patent.[35]

## Software Patents

A software patent claims as its invention some feature or process embodied in instructions executed by a computer. The courts and the USPTO have changed their attitudes and opinions on the patenting of software over the years. Prior to 1981, the courts regularly turned down requests for such patents, giving the impression that software could not be patented.[36]

In the 1981 *Diamond v. Diehr* case, the Supreme Court granted a patent to Diehr, who had developed a process control computer and sensors to monitor the temperature inside a rubber mold. The USPTO interpreted the court's reasoning to mean that just because an invention used software did not mean that the invention could not be patented. Based on this ruling, courts have slowly broadened the scope of protection for software-related inventions.[37] As a result, during the 1980s and 1990s, the USPTO granted thousands of software-related patents per year. Application software, business software, expert systems, and system software were patented, along with such software processes as compilation routines, editing and control functions, and operating system techniques. Many patents were granted for business methods implemented in software.

Starting in the latter half of the 2000s, the courts have become more restrictive on the granting of software patents.[38] Some software experts think that too many software patents are being granted, and they believe that this inhibits new software development.[39] Indeed, each new software patent lawsuit adds to the costs and business risks associated with

software development. During 2012, the following software patent battles were raging among some of the biggest names in the software industry:

- Oracle and Google battled over patent infringement claims associated with Oracle's Java programming language—with Oracle seeking $6 billion in damages.[40]
- Apple sued Samsung for patent infringement regarding several patents associated with Apple's smartphone and tablet devices. Apple was ultimately awarded $1.1 billion in damages.[41]
- Mformation, a global provider of mobile device management technology, was awarded $147 million when it sued Research in Motion for patent infringement of Mformation's patented technology, which enables companies to remotely access employee mobile phones to perform software upgrades, change passwords, and erase data.[42]
- Many industry observers believe that Google purchased Motorola Mobility, a smartphone software company, for $12.5 billion so that the firm could sue Apple over alleged infringement of patents associated with location reminders, email notification, and the Siri intelligent assistant.[43]



### Cross-Licensing Agreements

Many large software companies have cross-licensing agreements in which each party agrees not to sue the other over patent infringements. For example, Apple and HTC battled for several years over various mobile phone-related patents, which eventually led to the U.S. International Trade Committee banning imports of two models of the HTC mobile phone. The two companies eventually agreed to a 10-year cross-licensing agreement that permits each party to license the other's current and future patents.[44]

Major IT firms usually have little interest in cross-licensing with smaller firms. As a result, small businesses must pay an additional cost from which many larger companies are exempt. Furthermore, small businesses are generally unsuccessful in enforcing their patents against larger companies. Should a small business bring a patent infringement suit against a large firm, the larger firm can overwhelm the small business with multiple patent suits, whether they have merit or not. Considering that the average patent lawsuit costs $3 to $10 million and takes two to three years to litigate, a small firm often simply cannot afford to fight; instead, it usually settles and licenses its patents to the large company.[45]

## TRADE SECRETS

In Chapter 2, a trade secret was defined as business information that represents something of economic value, has required effort or cost to develop, has some degree of uniqueness or novelty, is generally unknown to the public, and is kept confidential.

Trade secret protection begins by identifying all the information that must be protected—from undisclosed patent applications to market research and business plans—and developing a comprehensive strategy for keeping the information secure. Trade secret law protects only against the *misappropriation* of trade secrets. If competitors come up with the same idea on their own, it is not misappropriation; in other words, the law doesn't prevent someone from using the same idea if it was developed independently.

software development. During 2012, the following software patent battles were raging among some of the biggest names in the software industry:

- Oracle and Google battled over patent infringement claims associated with Oracle's Java programming language—with Oracle seeking $6 billion in damages.[40]
- Apple sued Samsung for patent infringement regarding several patents associated with Apple's smartphone and tablet devices. Apple was ultimately awarded $1.1 billion in damages.[41]
- Mformation, a global provider of mobile device management technology, was awarded $147 million when it sued Research in Motion for patent infringement of Mformation's patented technology, which enables companies to remotely access employee mobile phones to perform software upgrades, change passwords, and erase data.[42]
- Many industry observers believe that Google purchased Motorola Mobility, a smartphone software company, for $12.5 billion so that the firm could sue Apple over alleged infringement of patents associated with location reminders, email notification, and the Siri intelligent assistant.[43]



### Cross-Licensing Agreements

Many large software companies have cross-licensing agreements in which each party agrees not to sue the other over patent infringements. For example, Apple and HTC battled for several years over various mobile phone-related patents, which eventually led to the U.S. International Trade Committee banning imports of two models of the HTC mobile phone. The two companies eventually agreed to a 10-year cross-licensing agreement that permits each party to license the other's current and future patents.[44]

Major IT firms usually have little interest in cross-licensing with smaller firms. As a result, small businesses must pay an additional cost from which many larger companies are exempt. Furthermore, small businesses are generally unsuccessful in enforcing their patents against larger companies. Should a small business bring a patent infringement suit against a large firm, the larger firm can overwhelm the small business with multiple patent suits, whether they have merit or not. Considering that the average patent lawsuit costs $3 to $10 million and takes two to three years to litigate, a small firm often simply cannot afford to fight; instead, it usually settles and licenses its patents to the large company.[45]

## TRADE SECRETS

In Chapter 2, a trade secret was defined as business information that represents something of economic value, has required effort or cost to develop, has some degree of uniqueness or novelty, is generally unknown to the public, and is kept confidential.

Trade secret protection begins by identifying all the information that must be protected—from undisclosed patent applications to market research and business plans—and developing a comprehensive strategy for keeping the information secure. Trade secret law protects only against the *misappropriation* of trade secrets. If competitors come up with the same idea on their own, it is not misappropriation; in other words, the law doesn't prevent someone from using the same idea if it was developed independently.

Trade secret laws protect more technology worldwide than patent laws do, in large part because of the following key advantages:

- There are no time limitations on the protection of trade secrets, as there are with patents and copyrights.
- There is no need to file an application, make disclosures to any person or agency, or disclose a trade secret to outsiders to gain protection. (After the USPTO issues a patent, competitors can obtain a detailed description of it.) Hence, no filing or application fees are required to protect a trade secret.
- Although patents can be ruled invalid by the courts, meaning that the affected inventions no longer have patent protection, this risk does not exist for trade secrets.



Fuhu is the creator of Nabi, an Android tablet computer for kids, that had been sold exclusively at Toys "R" Us stores. In a lawsuit filed in late 2012, Fuhu alleged that Toys "R" Us stole Nabi trade secrets during the year that the retailer served as the exclusive distributor of the product. As a result, Fuhu alleged, Toys "R" Us was able to bring out its competing tablet months ahead of schedule. Fuhu sued to stop the toy retailer from launching this rival tablet during the lucrative Christmas selling season.[46]

## Trade Secret Laws

Trade secret protection laws vary greatly from country to country. For example, the Philippines provides no legal protection for trade secrets. In some European countries, pharmaceuticals, methods of medical diagnosis and treatment, and information technology cannot be patented. Many Asian countries require foreign corporations operating there to transfer rights to their technology to locally controlled enterprises. (Coca-Cola reopened its operations in India in 1993 after halting sales for 16 years to protect the "secret formula" for its soft drink, even though India's vast population represented a huge potential market.) American businesses that seek to operate in foreign jurisdictions or enter international markets must take these differences into account.

### Uniform Trade Secrets Act (UTSA)

The Uniform Trade Secrets Act (UTSA) was drafted in the 1970s to bring uniformity to all the United States in the area of trade secret law. The first state to enact the UTSA was Minnesota in 1981, followed by 39 more states and the District of Columbia. The UTSA defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

- Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by, persons who can obtain economic value from its disclosure or use, and
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

Under these terms, computer hardware and software can qualify for trade secret protection by the UTSA.[47]

### The Economic Espionage Act (EEA) (1996)

The **Economic Espionage Act (EEA) of 1996** imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets. Before the EEA, there was no specific criminal statute to help pursue economic espionage; the FBI was investigating nearly 800 such cases in 23 countries when the EEA was enacted.[48] The Office of the National Counterintelligence Executive has estimated that the "combined costs of foreign and domestic economic espionage, including the theft of intellectual property, [are] as high as $300 billion per year and rising."[49] As with the UTSA, information is considered a trade secret under the EEA only if companies take steps to protect it.



DuPont is a major U.S.-based science and engineering company that has been in business since 1802.[50] The firm was a leader in research on Organic Light Emitting Diodes (OLED) that resulted in the development of a breakthrough and proprietary chemical process for OLED displays. However, a DuPont research chemist involved in the project stole trade secret compounds and passed them to a Chinese university. Ultimately, the chemist was caught by the FBI, prosecuted, and sentenced to 14 months in federal prison. The loss of the trade secrets was valued by DuPont at $400 million.[51]

## Employees and Trade Secrets

Employees are the greatest threat to the loss of company trade secrets—they might accidentally disclose trade secrets or steal them for monetary gain. Organizations must educate employees about the importance of maintaining the secrecy of corporate information. Trade secret information should be labeled clearly as confidential and should only be accessible by a limited number of people. Most organizations have strict policies regarding nondisclosure of corporate information.

Because organizations can risk losing trade secrets when key employees leave, they often try to prohibit employees from revealing secrets by adding **nondisclosure clauses** to employment contracts. Thus, departing employees cannot take copies of computer programs or reveal the details of software owned by the firm.

Defining reasonable nondisclosure agreements can be difficult, as seen in the following example involving Apple. In addition to filing hundreds of patents on iPhone technology, the firm put into place a restrictive nondisclosure agreement to provide an extra layer of protection. Many iPhone developers complained bitterly about the tough restrictions, which prohibited them from talking about their coding work with anyone not on the project team and even prohibited them from talking about the restrictions themselves. Eventually, Apple admitted that its nondisclosure terms were overly restrictive and loosened them for iPhone software that was already released.[52]

Another option for preserving trade secrets is to have an experienced member of the Human Resources Department conduct an exit interview with each departing employee. A key step in the interview is to review a checklist that deals with confidentiality issues. At the end of the interview, the departing employee is asked to sign an acknowledgment of responsibility not to divulge any trade secrets.

Employers can also use noncompete agreements to protect intellectual property from being used by competitors when key employees leave. A **noncompete agreement** prohibits an employee from working for any competitors for a period of time, often one to two years.

When courts are asked to settle disputes over noncompete agreements, they must weigh several factors. First, they must consider the reasonableness of the restriction and how it protects confidential and trade secret information of the former employer. Second, they must weigh the employee's right to work and seek employment in the area where the employee has gained skill, experience, and business contacts. The courts also consider geographic area and the length of time of the restriction in relation to the pace of change in the industry.



Most states only enforce such noncompete agreements to the extent required to shelter the employer's legitimate confidential business interests. However, there is a wide range of treatment on noncompete agreements among the various states. For example, Ohio is highly supportive of former employers enforcing noncompete agreements while noncompete agreements are seldom enforced in California.[53]

Electronic payments processing firm Vantiv filed a lawsuit alleging breach of a noncompete contract against its former senior vice president when he accepted a position with competitor iPayments. Vantiv hopes to bar the employee from working for the competitor and to gain return of a year's base salary received as part an employment termination agreement.[54] In another case, five software engineers brought a class action lawsuit against Apple, Google, Intel, Adobe Systems, Intuit, Pixar, and Lucasfilm alleging that the firms colluded to constrain salary and job mobility by maintaining do-not-call lists to avoid recruiting each other's employees. The engineers alleged that these agreements restrained competition and potentially cost the employees of these firms hundreds of millions of dollars.[55]

The following is an example of a typical, although not necessarily legally binding, noncompete agreement:

> The employee agrees as a condition of employment that in the event of termination for any reason, he or she will not engage in a similar or competitive business for a period of two years, nor will he or she contact or solicit any customer with whom Employer conducted business during his or her employment. This restrictive covenant shall be for a term of two years from termination, and shall encompass the geographic area within a 100-mile radius of Employer's place of business.

## KEY INTELLECTUAL PROPERTY ISSUES

This section discusses several issues that apply to intellectual property and information technology, including plagiarism, reverse engineering, open source code, competitive intelligence, trademark infringement, and cybersquatting.

### Plagiarism

**Plagiarism** is the act of stealing someone's ideas or words and passing them off as one's own. The explosion of electronic content and the growth of the Web have made it easy to cut and paste paragraphs into term papers and other documents without proper citation or quotation marks. To compound the problem, hundreds of online "paper mills" enable users to download entire term papers. Although some sites post warnings that their services should be used for research purposes only, many users pay scant heed. As a result, plagiarism has become an issue from elementary schools to the highest levels of academia.

Plagiarism also occurs outside academia. Popular literary authors, playwrights, musicians, journalists, and even software developers have been accused of it.

Despite codes of ethics in place that clearly define plagiarism and prescribe penalties ranging from no credit on a paper to expulsion, many students still do not understand what constitutes plagiarism. Some students believe that all electronic content is in the public domain, while other students knowingly commit plagiarism either because they feel pressure to achieve a high GPA or because they are too lazy or pressed for time to do original work.



A recent survey reported that 55 percent of university presidents felt that plagiarism has increased over the past decade in spite of increased efforts to combat the practice.[56] Plagiarism by students taking free online courses from Coursea has become so widespread that one professor felt compelled to post a request for his 39,000 students to stop the practice after many of the students complained about their fellow students.[57]

Some instructors say that being familiar with a student's style of writing, grammar, and vocabulary enables them to determine if the student actually wrote a paper. In addition, plagiarism detection systems (see Table 6-3) allow teachers, corporations, law firms, and publishers to check for matching text in different documents as a means of identifying potential plagiarism.

**TABLE 6-3** Partial list of plagiarism detection services and software

| Name of service | Web site | Provider |
|---|---|---|
| iThenticate | www.ithenticate.com | iParadigms |
| Turnitin | www.turnitin.com | iParadigms |
| SafeAssign | www.safeassign.com | Blackboard |
| Glatt Plagiarism Services | www.plagiarism.com | Glatt Plagiarism Services |
| EVE Plagiarism Detection | www.canexus.com/eve | CaNexus |

Source Line: Course Technology/Cengage Learning.

Turnitin, a software product developed by California-based iParadigms, supports 15 languages and is used by over 10,000 educational institutions around the world. It uses three primary databases for content matching with over 24 billion Web pages, some 300 million archived student papers, and 120 million articles from over 110,000 journals, periodicals, and books.[58] iThenticate is available from the same company that created Turnitin, but it is designed to meet the needs of members of the information industry, such as publishers, research facilities, legal firms, government agencies, and financial institutions.[59]

Interestingly, four high school students brought a lawsuit against iParadigms, accusing the firm of copyright infringement. The basis of their lawsuit was that the firm's primary product, Turnitin, used archived student papers without their permission to assess the originality of newly submitted papers. However, both a district court and a court of appeals ruled that the use of student papers for purposes of plagiarism detection constitutes a fair use and is therefore not a copyright infringement. A U.S. court of appeals ruled that such use of student papers "has a protective effect" on the future marketability of the

students' works and "provides a substantial public benefit through the network of institutions using Turnitin."[60]

The following list shows some of the actions that schools can take to combat student plagiarism:

- Help students understand what constitutes plagiarism and why they need to cite sources properly.
- Show students how to document Web pages and materials from online databases.
- Schedule major writing assignments so that portions are due over the course of the term, thus reducing the likelihood that students will get into a time crunch and be tempted to plagiarize to meet the deadline.
- Make clear to students that instructors are aware of Internet paper mills.
- Ensure that instructors both educate students about plagiarism detection services and make students aware that they know how to use these services.
- Incorporate detection software and services into a comprehensive antiplagiarism program.



## Reverse Engineering

**Reverse engineering** is the process of taking something apart in order to understand it, build a copy of it, or improve it. Reverse engineering was originally applied to computer hardware but is now commonly applied to software as well. Reverse engineering of software involves analyzing it to create a new representation of the system in a different form or at a higher level of abstraction. Often, reverse engineering begins by extracting design-stage details from program code. Design-stage details about an information system are more conceptual and less defined than the program code of the same system. Microsoft has been accused repeatedly of reverse engineering products—ranging from the Apple Macintosh user interface, to many Apple operating system utility features that were incorporated into DOS (and later Windows), to early word-processing and spreadsheet programs that set the design for Word and Excel, to Google's methods for improving search results for its Bing search engine.[61]

One frequent use of reverse engineering for software is to modify an application that ran on one vendor's database so that it can run on another's (for example, from Access to Oracle). Database management systems use their own programming language for application development. As a result, organizations that want to change database vendors are faced with rewriting existing applications using the new vendor's database programming language. The cost and length of time required for this redevelopment can deter an organization from changing vendors and deprive it of the possible benefits of converting to an improved database technology.

Using reverse engineering, a developer can use the code of the current database programming language to recover the design of the information system application. Next, code-generation tools can be used to take the design and produce code (forward engineer) in the new database programming language. This reverse-engineering and code-generating process greatly reduces the time and cost needed to migrate the organization's applications to the new database management system. No one challenges the right to use this process to convert applications developed in-house. After all, those applications were

developed and are owned by the companies using them. It is quite another matter, however, to use this process on a purchased software application developed and licensed by outside parties. Most IT managers would consider this action unethical because the software user does not actually own the right to the software. In addition, a number of intellectual property issues would be raised, depending on whether the software was licensed, copyrighted, or patented.

Other reverse-engineering issues involve tools called compilers and decompilers. A compiler is a language translator that converts computer program statements expressed in a source language (such as Java, C, C++, and COBOL) into machine language (a series of binary codes of 0s and 1s) that the computer can execute. When a software manufacturer provides a customer with its software, it usually provides the software in machine-language form. Tools called reverse-engineering compilers, or decompilers, can read the machine language and produce the source code. For example, REC (Reverse Engineering Compiler) is a decompiler that reads an executable, machine-language file and produces a C-like representation of the code used to build the program.



Decompilers and other reverse-engineering techniques can be used to reveal a competitor's program code, which can then be used to develop a new program that either duplicates the original or interfaces with the program. Thus, reverse engineering provides a way to gain access to information that another organization may have copyrighted or classified as a trade secret.

The courts have ruled in favor of using reverse engineering to enable interoperability. In the early 1990s, video game maker Sega developed a computerized lock so that only Sega video cartridges would work on its entertainment systems. This essentially shut out competitors from making software for the Sega systems. *Sega Enterprises Ltd. v. Accolade, Inc.* dealt with rival game maker Accolade's use of a decompiler to read the Sega software source code. With the code, Accolade could create new software that circumvented the lock and ran on Sega machines. An appeals court ultimately ruled that if someone lacks access to the unprotected elements of an original work and has a "legitimate reason" for gaining access to those elements, disassembly of a copyrighted work is considered to be a fair use under section 107 of the Copyright Act. The unprotected element in this case was the code necessary to enable software to interoperate with the Sega equipment. The court reasoned that to refuse someone the opportunity to create an interoperable product would allow existing manufacturers to monopolize the market, making it impossible for others to compete. This ruling had a major impact on the video game industry, allowing video game makers to create software that would run on multiple machines.

Software license agreements increasingly forbid reverse engineering. As a result of the increased legislation affecting reverse engineering, some software developers are moving their reverse-engineering projects offshore to avoid U.S. rules.

The ethics of using reverse engineering are debated. Some argue that its use is fair if it enables a company to create software that interoperates with another company's software or hardware and provides a useful function. This is especially true if the software's creator refuses to cooperate by providing documentation to help create interoperable software. From the consumer's standpoint, such stifling of competition increases costs and reduces business options. Reverse engineering can also be a useful tool in detecting software bugs and security holes.

Others argue strongly against the use of reverse engineering, saying it can uncover software designs that someone else has developed at great cost and taken care to protect. Opponents of reverse engineering contend it unfairly robs the creator of future earnings and significantly reduces the business incentive for software development.

## Open Source Code



Historically, the makers of proprietary software have not made their source code available, but not all developers share that philosophy. **Open source code** is any program whose source code is made available for use or modification, as users or other developers see fit. The basic premise behind open source code is that when many programmers can read, redistribute, and modify a program's code, the software improves. Programs with open source code can be adapted to meet new needs, and bugs can be rapidly identified and fixed. Open source code advocates believe that this process produces better software than the traditional closed model.

A considerable amount of open source code is available, and an increasing number of organizations use open source code. For example, much of the Internet runs on open source code; when you access a Web page, send a text, or post a status update, you are likely using open source code.[62]

A common use of open source software is to move data from one application to another and to extract, transform, and load business data into large databases. Two frequently cited reasons for using open source software are that it provides a better solution to a specific business problem and that it costs less. Open source software is used in applications developed for smartphones and other mobile devices, such as Apple's iPhone, Palm's Treo, and Research In Motion's BlackBerry. See Table 6-4 for a listing of commonly used open source software.

**TABLE 6-4** Commonly used open source software

| Open source software | Purpose |
|---|---|
| 7-Zip | File compression |
| Ares Galaxy | Peer-to-peer file sharing |
| Audacity | Sound editing and special effects |
| Azureus | Peer-to-peer file sharing |
| Blender 3D | 3D modeling and animation |
| eMule | Peer-to-peer file sharing |
| Eraser | Erasing data completely |
| Firefox | Internet browsing |
| OpenOffice | Word processing, spreadsheets, presentations, graphics, and databases |
| Video Dub | Video editing |

Source Line: Course Technology/Cengage Learning.

Why would firms or individual developers create open source code if they do not receive money for it? Here are several reasons:

- Some people share code to earn respect for solving a common problem in an elegant way.
- Some people have used open source code that was developed by others and feel the need to pay back by helping other developers.
- A firm may be required to develop software as part of an agreement to address a client's problem. If the firm is paid for the employees' time spent to develop the software rather than for the software itself, it may decide to license the code as open source and use it either to promote the firm's expertise or as an incentive to attract other potential clients with a similar problem.
- A firm may develop open source code in the hope of earning software maintenance fees if the end user's needs change in the future.
- A firm may develop useful code but may be reluctant to license and market it, and so might donate the code to the general public.



There are various definitions of what constitutes open source code, each with its own idiosyncrasies. The GNU General Public License (GPL) was a precursor to the open source code defined by the Open Source Initiative (OSI). GNU is a computer operating system composed entirely of free software; its name is a recursive acronym for GNUs Not Unix. The GPL is intended to protect GNU software from being made proprietary, and it lists terms and conditions for copying, modifying, and distributing free software. The OSI is a nonprofit organization that advocates for open source and certifies open source licenses. Its certification mark, "OSI Certified," may be applied only to software distributed under an open source license that meets OSI criteria, as described at its Web site, *www.opensource.org*.

A software developer could attempt to make a program open source simply by putting it into the public domain with no copyright. This would allow people to share the program and their improvements, but it would also allow others to revise the original code and then distribute the resulting software as their own proprietary product. Users who received the program in the modified form would no longer have the freedoms associated with the original software. Use of an open source license avoids this scenario.

## Competitive Intelligence

Competitive intelligence (as defined in Chapter 3) is legally obtained information that is gathered to help a company gain an advantage over its rivals. For example, some companies have employees who monitor the public announcements of property transfers to detect any plant or store expansions of competitors. An effective competitive intelligence program requires the continual gathering, analysis, and evaluation of data with controlled dissemination of useful information to decision makers. Competitive intelligence is often integrated into a company's strategic plan and executive decision making. According to a recent survey of 400 global companies with competitive intelligence programs, the number of companies that spend more than $1 million on this activity increased from 5 percent to 10 percent over the period 2007–2012.

Pharmaceutical companies represent 27 percent of the companies that spend more than $2 million on competitive intelligence.[63]

Competitive intelligence is used to support smart business decisions in many different areas. For example, a European sporting goods manufacturer wanted to enter the U.S. market and was looking for good entry opportunities. Gathering and analyzing data about its competitors, the firm discovered an overlooked and rapidly growing market—wrestling headgear and apparel for girls.[64]



Competitive intelligence is not the same as **industrial espionage**, which is the use of illegal means to obtain business information not available to the general public. In the United States, industrial espionage is a serious crime that carries heavy penalties.

Almost all the data needed for competitive intelligence can be collected from examining published information or interviews, as outlined in the following list:

- 10-K or annual reports
- An SC 13D acquisition—a filing by shareholders who report owning more than 5 percent of common stock in a public company
- 10-Q or quarterly reports
- Press releases
- Promotional materials
- Web sites
- Analyses by the investment community, such as a Standard & Poor's stock report
- Dun & Bradstreet credit reports
- Interviews with suppliers, customers, and former employees
- Calls to competitors' customer service groups
- Articles in the trade press
- Environmental impact statements and other filings associated with a plant expansion or construction
- Patents

By coupling this competitive intelligence data with analytical tools and industry expertise, an experienced analyst can make deductions that lead to significant information. According to Avinash Kaushik, self-described "analytics evangelist" for Google, "The Web is the best competitive intelligence tool in the world." Kaushik likens the failure to use such data to driving a car 90 miles an hour with the windshield painted black, then scraping off the paint and realizing "you're going 90 but everyone else is going 220 and you're going to die."

A wide array of software applications, databases, and social media tools are available for companies—and individuals—looking for competitive intelligence data, including the following:

- Rapportive is software that can be added to your email application or Web browser to provide you with rich contact profiles that show you what people look like, where they are based, and what they do. Such information can help you build rapport quickly by enabling you to mention shared interests.
- Crunchbase is a free database of technology of over 110,000 companies, people, and investors.

- CORI (*http://cori.missouri.edu/pages/ksearch.htm*) is a database of contract documents available online using a full-text search and retrieval system.
- ThomasNet.com is an excellent source for identifying suppliers and sources for products.
- WhoGotFunded.com is a comprehensive Web site of data about what organizations have received funding and for what purposes.

Competitive intelligence gathering has become enough of a science that over two dozen colleges and universities offer courses or even entire programs in this subject. Also, the Strategic and Competitive Intelligence Professionals organization (*www.scip.org*) offers ongoing training programs and conferences.



Without proper management safeguards, the process of gathering competitive intelligence can cross over to industrial espionage and dirty tricks. One frequently used dirty trick is to enter a bar near a competitor's plant or headquarters, strike up a conversation, and ply people for information after their inhibitions have been weakened by alcohol.

Competitive intelligence analysts must avoid unethical or illegal actions, such as lying, misrepresentation, theft, bribery, or eavesdropping with illegal devices. Table 6-5 provides a manager's checklist for running an ethical competitive intelligence operation. The preferred answer to each question in the checklist is *yes*.

**TABLE 6-5** A manager's checklist for running an ethical competitive intelligence operation

| Question | Yes | No |
|---|---|---|
| Has the competitive intelligence organization developed a mission statement, objectives, goals, and a code of ethics? | | |
| Has the company's legal department approved the mission statement, objectives, goals, and code of ethics? | | |
| Do analysts understand the need to abide by their organization's code of ethics and corporate policies? | | |
| Is there a rigorous training and certification process for analysts? | | |
| Do analysts understand all applicable laws—domestic and international—including the Uniform Trade Secrets Act and the Economic Espionage Act, and do they understand the critical importance of abiding by them? | | |
| Do analysts disclose their true identity as well as the name of their organization prior to any interviews? | | |
| Do analysts understand that everything their firm learns about the competition must be obtained legally? | | |
| Do analysts respect all requests for anonymity and confidentiality of information? | | |
| Has the company's legal department approved the processes for gathering data? | | |
| Do analysts provide honest recommendations and conclusions? | | |
| Is the use of third parties to gather competitive intelligence carefully reviewed and managed? | | |

Source Line: Course Technology/Cengage Learning.