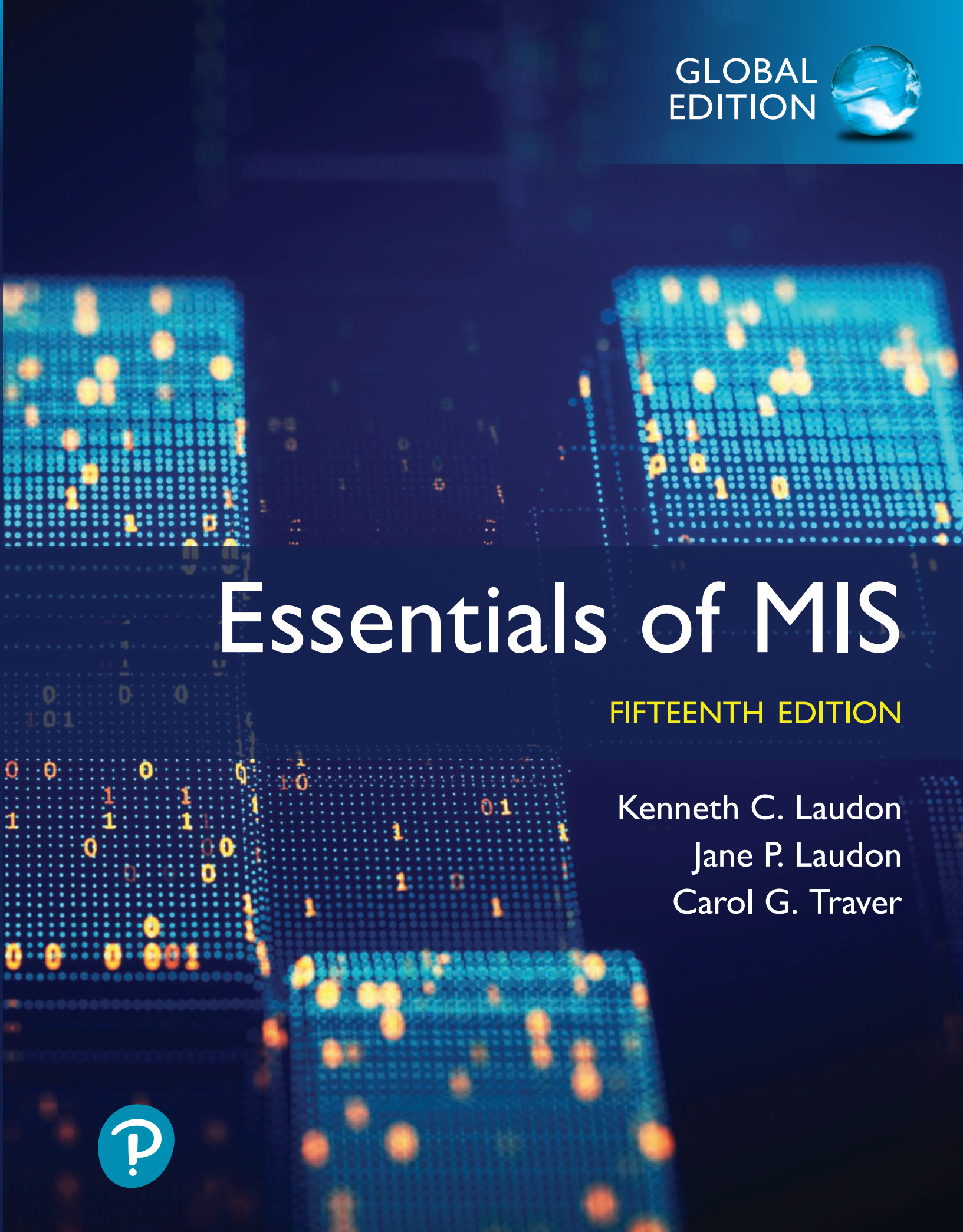
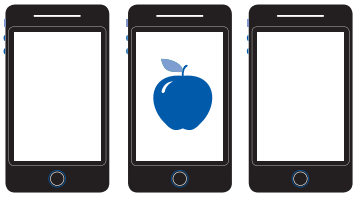



# Essentials of MIS

FIFTEENTH EDITION

Kenneth C. Laudon
Jane P. Laudon
Carol G. Traver

- **Dynamic Study Modules** help students study chapter topics and the language of MIS on their own by continuously assessing their knowledge application and performance in real time. These are available as graded assignments prior to class, and are accessible on smartphones, tablets, and computers.



- **Learning Catalytics™** is a student response tool that helps you generate class discussion, customize your lecture, and promote peer-to-peer learning based on real-time analytics. Learning Catalytics uses students' smartphones, tablets, or laptops to engage them in more interactive tasks.

- The **Gradebook** offers an easy way for you and your students to see their performance in your course.

  Item Analysis lets you quickly see trends by analyzing details like the number of students who answered correctly/incorrectly, time on task, and more.

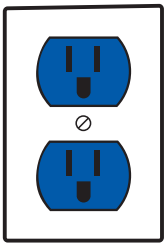
  And because it's correlated with the AACSB Standards, you can track students' progress toward outcomes that the organization has deemed important in preparing students to be leaders.

- **Pearson eTextbook** enhances learning—both in and out of the classroom. Students can take notes, highlight, and bookmark important content, or engage with interactive lecture and example videos that bring learning to life anytime, anywhere via MyLab or the app.

- **Accessibility (ADA)**—Pearson is working toward WCAG 2.0 Level AA and Section 508 standards, as expressed in the **Pearson Guidelines for Accessible Educational Web Media.** Moreover, our products support customers in meeting their obligation to comply with the Americans with Disabilities Act (ADA) by providing access to learning technology programs for users with disabilities.

  Please email our Accessibility Team at **disability.support@pearson.com** for the most up-to-date information.

- With **LMS Integration**, you can link your MyLab course from Blackboard Learn™, Brightspace® by D2L®, Canvas™, or Moodle®.



http://www.pearsonmylabandmastering.com

**TABLE 4.4**

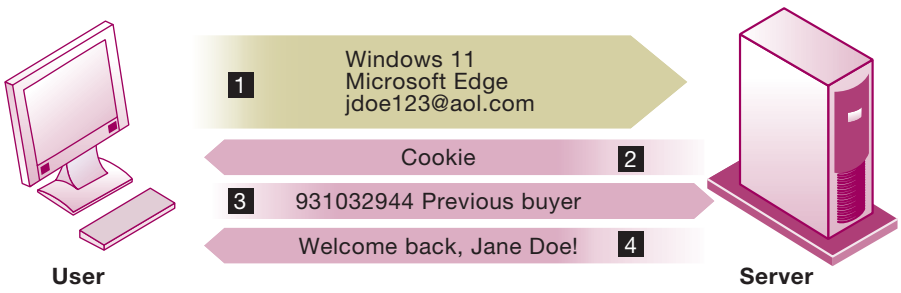
Examples of Privacy Laws in Various Nations

| Nation | Privacy |
|---|---|
| Australia | The Australia Privacy Principles (APPs) establish the privacy protection framework in the Privacy Act of 1988. The APPs consist of 13 principles guiding the handling of personal information in an open and clear manner. Privacy policies detail why and how personal information is collected, how individuals can access and correct their own information, and how individuals can complain about a breach of the principles. The APPs apply to most Australian government agencies and some private sector organizations. The APPs are principles-based laws that give an organization flexibility in tailoring their personal information handling practices to their business models and the diverse needs of individuals. A breach of an APP can lead to regulatory action and penalties. |
| Iceland | Iceland is not a member of the EU but has close ties as a party to the European Economic Area Agreement. Iceland is obligated to incorporate specific EU acts into Icelandic national legislation and has implemented the EU GDPR through its Data Protection Act. Iceland's Data Protection Authority (DPA) is authorized to impose administrative fines for breaches of GDPR and Data Protection Act provisions. A significant breach of the Data Protection Act (such as when the PII of a large number of data subjects that should have remained confidential is deliberately transferred to a third party or published publicly) can result in up to a three-year prison sentence. |
| Singapore | The Personal Data Protection Act (DPA) of 2012 provides various rules governing the collection, use, disclosure, and care of personal data. DPA stipulates that personal information may only be collected for reasonable purposes and with the consent of the individual, who must also be informed of the purpose for the data collection. There are some exceptions. (For example, DPA exempts personal data processed by an individual for the purposes of their personal, family or household affairs. Police or taxation authorities do not have to disclose information held or processed to prevent crime or taxation fraud.) |
| South Africa | Protection of personal data is addressed by the Electronic Communications and Transactions Act of 2002, which provides for the facilitation and regulation of electronic communications and transactions, including protection of personal information. Subscription to the ECT Act's regime for protecting PII is voluntary. Collectors of PII may subscribe to a set of universally accepted data protection principles. It is envisaged that individuals will prefer to deal only with the data collectors that have subscribed to ECT Act data protection principles. Sanctions for breaching ECT Act provisions are left to the participating parties themselves to agree on. |

## Internet Challenges to Privacy

Internet technology poses new challenges for the protection of individual privacy. It enables companies to track web searches that users conduct, the websites and web pages visited, the online content a person has accessed, and what items that person has inspected or purchased online. Mobile apps can also track users. This monitoring and tracking occurs in the background without the visitor's knowledge. It is conducted not just by individual websites (known as first-party tracking) but by advertising networks such as Microsoft Advertising, Google's Marketing Platform, and Meta's Audience Network that are capable of tracking personal browsing behavior across thousands of websites (known as third-party tracking). In the past, website publishers and the online advertising industry have defended tracking of individuals across the web because doing so allows more relevant ads to be targeted to users, and this helps pay for the cost of providing online content. The commercial demand for this personal information is virtually insatiable. However, these practices also impinge on individual privacy.

**Cookies** are one method used to monitor and track online users. Examine Figure 4.3, which illustrates how cookies work. When a user visits a website, the website's web server places a small text file (a "cookie") on the user's computer or mobile device. Cookies identify the visitor's web browser software, as well as other information, and track visits to the website. When the visitor returns to a site that has stored




1. The web server reads the user's web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer.
3. When the user returns to the website, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The web server reads the cookie, identifies the visitor, and calls up data on the user.

**Figure 4.3**
How First-Party Cookies Identify Web Visitors
*Cookies are placed by a website on a visitor's computer. When the visitor returns to that website, the web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The website can then use these data to display personalized information.*

a cookie, the website software searches the visitor's computer or mobile device, finds the cookie, and knows what that person has done in the past. It may also update the cookie, depending on the activity during the visit. In this way, the site can customize its content for each visitor's interests. For example, if you purchase a book on Amazon.com and return later from the same browser, the site will welcome you by name and recommend other books of interest based on your past purchases. Cookies also make "quick checkout" options possible by allowing a site to keep track of users as they add items to a shopping cart. This type of cookie is known as a first-party cookie. First-party cookies are typically considered to be "good" cookies because they help enhance the user experience.

Websites using cookie technology cannot directly obtain visitors' names and addresses. However, if a person has registered at a site, that information can be combined with cookie data to identify the visitor. Website owners can also combine the data they have gathered from cookies and other website monitoring tools with personal data from other sources, such as offline data collected from surveys or paper catalog purchases, to develop very detailed profiles of their visitors. First-party cookies can be blocked and/or deleted by users, although the majority of users do not do so.

Third-party cookies operate similarly to first-party cookies but enable advertising platforms to track user behavior across websites and devices. In the past, third-party cookies were supported by all the major web browsers, but that has begun to change. Apple's Safari and Mozilla's Firefox browsers now block third-party cookies by default, and Google has announced that it will follow suit beginning in 2024. We discuss other technology-based efforts to enhance privacy in the following section on technological solutions.

In addition to cookies, there are other tools for surveillance of Internet users. A **web beacon**, also called a *web bug* (or simply tracking file), is a tiny image that keeps a record of users' online clickstreams. They report these data back to whoever owns the tracking file, which can be invisibly embedded in an email message or web page to monitor the behavior of the user visiting the website or receiving the email. Web beacons are placed on popular websites by third-party firms who pay the websites a fee for access to their audience. So how common is web tracking? In a path-breaking series of articles in the *Wall Street Journal*, researchers examined the tracking files on 50 of the most popular US websites. What they found revealed a very widespread surveillance system: On the 50 sites, they discovered 3,180 tracking files installed on visitor computers. Only one site, Wikipedia, had no tracking files. Two-thirds of the tracking files came from 131 companies whose primary business is identifying and tracking Internet users to create consumer profiles that can be sold to advertising firms looking for specific types of customers. The biggest trackers were Google,

Microsoft, and Quantcast, all of whom are in the business of selling ads to advertising firms and marketers. A follow-up study found tracking on the 50-most-popular sites had risen nearly fivefold because of the growth of online ad auctions where advertisers buy the data about users' web-browsing behaviors.

**Adware** can secretly install itself on an Internet user's computer by piggybacking on larger applications. Once installed, adware calls out to websites to send ads and other unsolicited material to the user. A more malicious version of adware, known as **spyware** can also track the user's browsing habits. More information is available about intrusive software in Chapter 8.

More than 90 percent of global Internet users use Google Search and other Google services, making Google the world's largest collector of online user data. Whatever Google does with its data has an enormous impact on online privacy. Most experts believe that Google possesses the largest collection of personal information in the world—more data on more people than any government agency. Google uses behavioral targeting (also known as interest-based advertising) to target individuals as they move from one site to another to show them relevant ads based on their search activities and other data that Google has collected about them. For instance, one of its programs enables advertisers to target ads based on the search histories of Google users, along with any other information the user submits to Google such as age, demographics, region, and web activities (such as blogging). Google's AdSense program enables Google to help advertisers select keywords and design ads for various market segments based on search histories such as helping a clothing website create and test ads targeted at teenage females. Google displays targeted ads on YouTube and Google mobile applications, and its Google Marketing Platform ad network serves targeted ads.

The United States has allowed businesses to gather transaction information generated in the marketplace and then use that information for other marketing purposes without obtaining the **informed consent** of the individual whose information is being used. These firms argue that when users agree to the sites' terms of service, they are also agreeing to allow the site to collect information about their online activities. An **opt-out** model of informed consent permits the collection of personal information until the consumer specifically requests the data not to be collected. Privacy advocates would like to see wider use of an **opt-in** model of informed consent in which a business is prohibited from collecting any personal information unless the consumer specifically takes action to approve information collection and use. Here, the default option is no collection of user information. Many websites now employ "cookie banners"—a pop-up window that allows users to accept or reject cookies from the site. Although intended as a form of opt-in informed consent, most privacy advocates feel that cookie banners are ineffective, as few people actually read the disclosures about what data are being collected before clicking the Accept button.

The online industry has preferred self-regulation to privacy legislation for protecting consumers. Members of the online advertising industry have created an industry association called the Network Advertising Initiative (NAI) to develop privacy policies to help consumers opt out of advertising network programs and to provide consumers redress from abuses. Individual firms such as Apple, Google, and Microsoft have also launched privacy initiatives in an effort to address public concern about tracking people online.

In general, most businesses do little to protect the privacy of their customers, and consumers do not do as much as they should to protect themselves. For websites and apps that depend on advertising for support, most revenue derives from selling access to customer information. The vast majority of people claim to be concerned about online privacy, but most do not read the privacy statements on websites. In addition, website privacy policies are often ambiguous about key terms and too complicated for the average consumer to understand (Laudon and Traver, 2024). What firms call

**TABLE 4.5**

Technological Protections for Online Privacy

| Technology | Protection |
|---|---|
| Apple App Tracking Transparency (ATT) | Requires any app that wants to track user activity and share it with other apps or websites to ask user for permission |
| Apple Intelligent Tracking Prevention (ITP) for Safari web browser | Monitors and disables cross-site tracking cookies and blocks trackers' ability to identify users by IP address |
| Google Privacy Sandbox | System now being tested by Google to replace cookie-based, targeted advertising in the Google Chrome web browser by 2024 |
| Differential privacy software | Reduces the ability to merge different files and de-anonymize consumer data |
| Privacy default browsers | Eliminates tracking cookies and prevents IP tracking |
| Message encryption apps | Encrypts text and other data transferred using smartphones |
| Spyware blockers | Detects and removes spyware, adware, keyloggers, and other malware |
| Pop-up and ad blockers | Prevents calls to ad servers; restricts downloading of images at user request |
| Secure email | Email and document encryption |
| Anonymous remailers | Enhanced privacy protection for email |
| Anonymous surfing | Enhanced privacy protection for web browsing |
| Cookie managers | Blocks third-party cookies |
| Public key encryption | Enables encryption of email and documents |

a privacy policy is in fact a data use policy. The concept of privacy is associated with consumer rights, which many firms do not wish to recognize. A data use policy simply tells customers how the information will be used and does not mention rights.

### Technological Solutions

In addition to legislation, a number of technological solutions have been developed to help protect user privacy. Table 4.5 lists some of the most common tools that are available. For the most part, technical solutions thus far have failed to provide effective protection for online privacy, in part because most of them require users to be proactive in implementing them.

## PROPERTY RIGHTS: INTELLECTUAL PROPERTY

Contemporary information systems have severely challenged existing laws and social practices that protect **intellectual property**. Intellectual property refers to products of the mind created by individuals or corporations. Information technology has made it difficult to protect intellectual property because digital information can be so easily copied or distributed. Intellectual property is subject to a variety of protections under four legal traditions: copyright, patents, trademarks, and trade secrets.

### Copyright

**Copyright** protects creators of intellectual property from having their work copied by others for any purpose for a certain period of time, depending on several factors. As a general rule, U.S. copyright protection lasts for the life of the author, plus an additional 70 years after the author's death. For corporate-owned works, copyright

protection generally lasts for 95 years after initial creation. Copyright protects literary, dramatic, musical, and artistic works, such as novels, poetry, songs, plays, maps, drawings, and artwork. The intent behind copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work. Most industrial nations have their own copyright laws, and there are several international conventions and bilateral agreements through which nations coordinate and enforce their copyright laws.

In the mid-1960s, the Copyright Office began registering software programs, and in 1980, Congress passed the Computer Software Copyright Act, which provides protection for software program code and copies of the original code sold in commerce; it sets forth the rights of the purchaser to use the software, while the creator retains legal title.

Copyright protects against copying entire programs or their parts. Damages and relief are readily obtained for infringement. The drawback to copyright protection is that the underlying ideas behind a work are not protected; only their manifestation in a work are protected. A competitor can use your software, understand how it works, and build new software that follows the same concepts without infringing on a copyright.

## Patents

A U.S. **patent** grants the owner an exclusive monopoly on the ideas behind an invention for a certain period of time, typically 20 years. The key concepts in patent law are originality, novelty, and invention. The granting of a patent is determined by the United States Patent and Trademark Office and relies on court rulings. In Europe, patents can be obtained directly from particular countries under the terms of specific national laws or via a central process enabled by the European Patent Convention, which harmonized many of the national laws to a certain extent.

The danger of patents is that they may stifle competition by raising barriers to entry into an industry. Patents force new entrants to pay licensing fees to patent owners and therefore can slow down the development of technical applications of new ideas.

## Trademarks

**Trademarks** are the marks, symbols, and images used to distinguish products in the marketplace. Trademark laws protect consumers by ensuring that they receive what they paid for. These laws also protect the investments that firms have made to bring products to market. Typical trademark infringement violations occur when one firm appropriates or pirates the marks of a competing firm. Infringement also occurs when firms dilute the value of another firm's marks by weakening the connection between a mark and the product. For instance, if a firm copies the trademarked Google icon, colors, and images, it would be infringing on Google's trademarks. It would also be diluting the connection between the Google search service and its trademarks, potentially creating confusion in the marketplace.

ICANN has a set of procedures to rapidly resolve trademark disputes regarding domain names called the Uniform Rapid Suspension (URS) system. These include a procedure that allows a trademark owner to seek suspension of an infringing domain name and a Trademark Clearing house repository of data on registered, court-validated, or statute-protected trademarks.

## Trade Secrets

Any intellectual work product—a formula, device, pattern, or compilation of data—used for a business purpose can be classified as a **trade secret**, provided that it is not based on information in the public domain. Protections for trade secrets vary from state to state. In general, trade secret laws grant a monopoly on the ideas behind a work product, but the monopoly can be very tenuous.

Software that contains novel or unique elements, procedures, or compilations can be considered a trade secret. Trade secret law protects the actual ideas in a work product, not only their manifestation. To make a claim of trade secret infringement, the creator or owner must take care to bind employees and customers with nondisclosure agreements and prevent the secret from falling into the public domain.

The limitation of trade secret protection is that although virtually all software programs of any complexity contain unique elements of some sort, it is difficult to prevent the ideas in the work from falling into the public domain when the software is widely distributed.

## Challenges to Intellectual Property Rights

Contemporary information technologies, especially software, pose severe challenges to existing methods of protecting intellectual property and, therefore, create significant ethical, social, and political issues. Digital media differ from books, periodicals, and other media in terms of the former's ease of replication; ease of transmission; ease of alteration; ease of theft because of compactness; and difficulties in establishing uniqueness.

The proliferation of digital networks, including the Internet, has made it even more difficult to protect intellectual property. Before the widespread use of digital networks, copies of software, books, magazine articles, or films had to be stored on physical media such as paper, computer disks, or videotape, creating some hurdles to distribution. Using digital networks, information can be more widely reproduced and distributed. A Global Software Survey conducted by International Data Corporation and BSA/The Software Alliance reported that 37 percent of the software installed on personal computers was unlicensed. Software piracy remains an ongoing issue, with the number of visits to software piracy sites worldwide increasing to 3.2 billion in 2021 (BSA/The Software Alliance, 2018; Statista Research Department, 2021).

The Internet was designed to transmit information, including copyrighted information, freely around the world. You can easily copy and distribute virtually anything to millions of people worldwide even if they are using different types of computer systems. Information can also be illicitly copied from one place and distributed throughout other systems and networks even though these parties do not willingly participate in the infringement.

Individuals have been illegally copying and distributing digitized music files on the Internet for several decades. Illegal file sharing became so widespread that it threatened the viability of the music recording industry and, at one point, consumed 20 percent of Internet bandwidth. The recording industry won several legal battles for shutting these services down, but it has not been able to halt illegal file sharing entirely. The motion picture and cable television industries continue to wage similar battles. Several European nations have worked with US authorities to shut down illegal sharing sites, with mixed results.

However, as legitimate online music stores such as iTunes and streaming services such as Spotify, Apple Music, Amazon Prime Music, and Pandora have expanded, illegal file sharing has significantly declined. The Apple iTunes Store legitimized paying for music and entertainment and created a closed environment from which music and videos could not be easily copied and widely distributed. Amazon's Kindle also protects the rights of publishers and writers because its books cannot be copied to the Internet and distributed. Music and video streaming services also inhibit piracy because the streams cannot be easily recorded on separate devices. Since 2015, music industry revenues have more than doubled after a precipitous drop of more than 50 percent between 1999 and 2014.

The **Digital Millennium Copyright Act (DMCA)** also provides some copyright protection. The DMCA implemented a World Intellectual Property Organization Treaty that makes it illegal to circumvent technology-based protections of copyrighted