TABLE 1.1 MAJOR TRENDS IN E-COMMERCE 2016–2017

BUSINESS

- Retail e-commerce in the United States continues double-digit growth (over 15%), with global growth rates even higher in Europe and emerging markets such as China, India, and Brazil.
- Mobile e-commerce (both retail and travel sales) explodes and is estimated to reach over $180 billion in the United States in 2016.
- The mobile app ecosystem continues to grow, with over 210 million Americans using mobile apps.
- Social e-commerce, based on social networks and supported by advertising, emerges and continues to grow, generating $3.9 billion in revenue for the top 500 social media retailers in the United States in 2015.
- Local e-commerce, the third dimension of the mobile, social, local e-commerce wave, also is growing in the United States, fueled by an explosion of interest in on-demand services such as Uber, to over $40 billion in 2016.
- B2B e-commerce in the United States continues to strengthen and grow to $6.7 trillion.
- On-demand service firms like Uber and Airbnb attract billions in capital, garner multi-billion dollar valuations, and show explosive growth.
- Mobile advertising continues growing at astronomical rates, accounting for almost two-thirds of all digital ad spending.
- Small businesses and entrepreneurs continue to flood into the e-commerce marketplace, often riding on the infrastructures created by industry giants such as Apple, Facebook, Amazon, Google, and eBay.

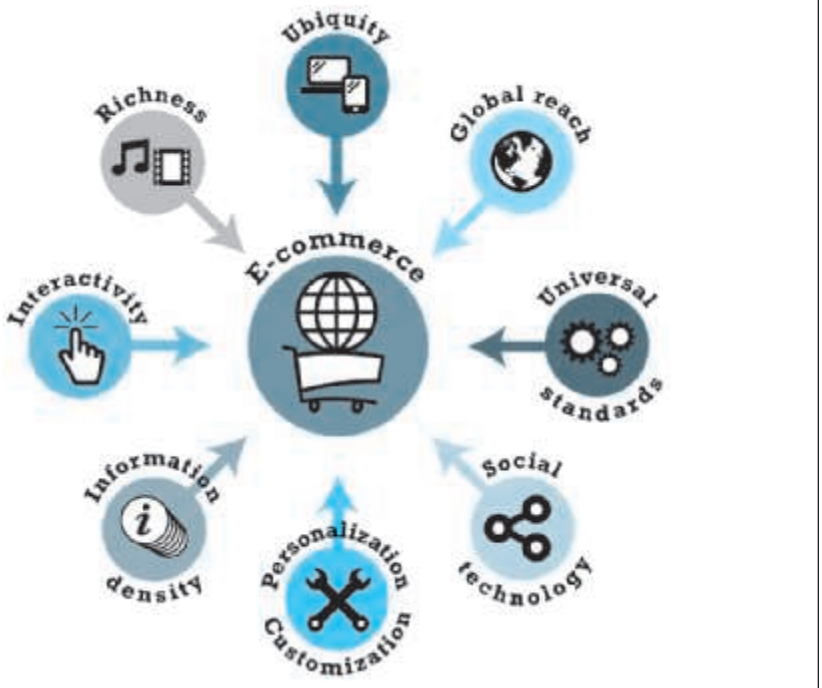
TECHNOLOGY

- A mobile computing and communications platform based on smartphones, tablet computers, wearable devices, and mobile apps becomes a reality, creating an alternative platform for online transactions, marketing, advertising, and media viewing. The use of mobile messaging services such as WhatsApp and Snapchat continues to expand, and these services are now used by over 60% of smartphone users.
- Cloud computing completes the transformation of the mobile platform by storing consumer content and software on "cloud" (Internet-based) servers and making it available to any consumer-connected device from the desktop to a smartphone.
- The Internet of Things, comprised of billions of Internet-connected devices, continues to grow exponentially.
- As firms track the trillions of online interactions that occur each day, a flood of data, typically referred to as big data, is being produced.
- In order to make sense out of big data, firms turn to sophisticated software called business analytics (or web analytics) that can identify purchase patterns as well as consumer interests and intentions in milliseconds.

SOCIETY

- User-generated content, published online as social network posts, tweets, blogs, and pins, as well as video and photo-sharing, continues to grow and provides a method of self-publishing that engages millions.
- The amount of data the average American consumes continues to increase, more than doubling from an average of about 34 gigabytes in 2008 to an estimated 74 gigabytes today.
- Social networks encourage self-revelation, while threatening privacy.
- Participation by adults in social networks increases; Facebook becomes ever more popular in all demographic categories.
- Conflicts over copyright management and control continue, but there is substantial agreement among online distributors and copyright owners that they need one another.
- Taxation of online sales becomes more widespread.
- Surveillance of online communications by both repressive regimes and Western democracies grows.
- Concerns over commercial and governmental privacy invasion increase.
- Online security continues to decline as major sites are hacked and lose control over customer information.
- Spam remains a significant problem despite legislation and promised technology fixes.
- On-demand service e-commerce produces a flood of temporary, poorly paid jobs without benefits.

FIGURE 1.4 EIGHT UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY



E-commerce technologies provide a number of unique features that have impacted the conduct of business.

1.3 UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY

Figure 1.4 illustrates eight unique features of e-commerce technology that both challenge traditional business thinking and help explain why we have so much interest in e-commerce. These unique dimensions of e-commerce technologies suggest many new possibilities for marketing and selling—a powerful set of interactive, personalized, and rich messages are available for delivery to segmented, targeted audiences.

Prior to the development of e-commerce, the marketing and sale of goods was a mass-marketing and salesforce–driven process. Marketers viewed consumers as passive targets of advertising campaigns and branding "blitzes" intended to influence their long-term product perceptions and immediate purchasing behavior. Companies sold their products via well-insulated channels. Consumers were trapped by geographical and social boundaries, unable to search widely for the best price and quality. Information about prices, costs, and fees could be hidden from the consumer, creating profitable information asymmetries for the selling firm. **Information asymmetry** refers to any disparity in relevant market information among parties in a transaction. It was so expensive to change national or regional prices in traditional retailing (what are called *menu costs*) that one national price was the norm, and dynamic pricing to

information asymmetry
any disparity in relevant market information among parties in a transaction

the marketplace (changing prices in real time) was unheard of. In this environment, manufacturers prospered by relying on huge production runs of products that could not be customized or personalized.

E-commerce technologies make it possible for merchants to know much more about consumers and to be able to use this information more effectively than was ever true in the past. Online merchants can use this information to develop new information asymmetries, enhance their ability to brand products, charge premium prices for high-quality service, and segment the market into an endless number of subgroups, each receiving a different price. To complicate matters further, these same technologies also make it possible for merchants to know more about other merchants than was ever true in the past. This presents the possibility that merchants might collude on prices rather than compete and drive overall average prices up. This strategy works especially well when there are just a few suppliers (Varian, 2000a). We examine these different visions of e-commerce further in Section 1.4 and throughout the book.

Each of the dimensions of e-commerce technology illustrated in Figure 1.4 deserves a brief exploration, as well as a comparison to both traditional commerce and other forms of technology-enabled commerce.

UBIQUITY

marketplace
physical space you visit in order to transact

ubiquity
available just about everywhere, at all times

marketspace
marketplace extended beyond traditional boundaries and removed from a temporal and geographic location

In traditional commerce, a **marketplace** is a physical place you visit in order to transact. For example, television and radio typically motivate the consumer to go someplace to make a purchase. E-commerce, in contrast, is characterized by its **ubiquity**: it is available just about everywhere, at all times. It liberates the market from being restricted to a physical space and makes it possible to shop from your desktop, at home, at work, or even from your car, using mobile e-commerce. The result is called a **marketspace**—a marketplace extended beyond traditional boundaries and removed from a temporal and geographic location.

From a consumer point of view, ubiquity reduces *transaction costs*—the costs of participating in a market. To transact, it is no longer necessary that you spend time and money traveling to a market. At a broader level, the ubiquity of e-commerce lowers the cognitive energy required to transact in a marketspace. *Cognitive energy* refers to the mental effort required to complete a task. Humans generally seek to reduce cognitive energy outlays. When given a choice, humans will choose the path requiring the least effort—the most convenient path (Shapiro and Varian, 1999; Tversky and Kahneman, 1981).

GLOBAL REACH

E-commerce technology permits commercial transactions to cross cultural, regional, and national boundaries far more conveniently and cost-effectively than is true in traditional commerce. As a result, the potential market size for e-commerce merchants is roughly equal to the size of the world's online population (an estimated 3.3 billion in 2016) (eMarketer, Inc., 2016d). More realistically, the Internet makes it much easier for startup e-commerce merchants within a single country to achieve a national audience than was ever possible in the past. The total number of users or

customers an e-commerce business can obtain is a measure of its **reach** (Evans and Wurster, 1997).

reach
the total number of users or customers an e-commerce business can obtain

In contrast, most traditional commerce is local or regional—it involves local merchants or national merchants with local outlets. Television, radio stations, and newspapers, for instance, are primarily local and regional institutions with limited but powerful national networks that can attract a national audience. In contrast to e-commerce technology, these older commerce technologies do not easily cross national boundaries to a global audience.

UNIVERSAL STANDARDS

One strikingly unusual feature of e-commerce technologies is that the technical standards of the Internet, and therefore the technical standards for conducting e-commerce, are **universal standards**—they are shared by all nations around the world. In contrast, most traditional commerce technologies differ from one nation to the next. For instance, television and radio standards differ around the world, as does cell phone technology.

universal standards
standards that are shared by all nations around the world

The universal technical standards of e-commerce greatly lower *market entry costs*—the cost merchants must pay just to bring their goods to market. At the same time, for consumers, universal standards reduce *search costs*—the effort required to find suitable products. And by creating a single, one-world marketspace, where prices and product descriptions can be inexpensively displayed for all to see, *price discovery* becomes simpler, faster, and more accurate (Banerjee et al., 2005; Bakos, 1997; Kambil, 1997). Users, both businesses and individuals, also experience *network externalities*—benefits that arise because everyone uses the same technology. With e-commerce technologies, it is possible for the first time in history to easily find many of the suppliers, prices, and delivery terms of a specific product anywhere in the world, and to view them in a coherent, comparative environment. Although this is not necessarily realistic today for all or even most products, it is a potential that will be exploited in the future.

RICHNESS

Information **richness** refers to the complexity and content of a message (Evans and Wurster, 1999). Traditional markets, national sales forces, and retail stores have great richness: they are able to provide personal, face-to-face service using aural and visual cues when making a sale. The richness of traditional markets makes them a powerful selling or commercial environment. Prior to the development of the Web, there was a trade-off between richness and reach: the larger the audience reached, the less rich the message.

richness
the complexity and content of a message

E-commerce technologies have the potential for offering considerably more information richness than traditional media such as printing presses, radio, and television because they are interactive and can adjust the message to individual users. Chatting with an online sales person, for instance, comes very close to the customer experience in a small retail shop. The richness enabled by e-commerce technologies allows retail and service merchants to market and sell "complex" goods and services that heretofore required a face-to-face presentation by a sales force to a much larger audience.

INTERACTIVITY

interactivity
technology that allows for two-way communication between merchant and consumer

Unlike any of the commercial technologies of the twentieth century, with the possible exception of the telephone, e-commerce technologies allow for **interactivity**, meaning they enable two-way communication between merchant and consumer and among consumers. Traditional television or radio, for instance, cannot ask viewers questions or enter into conversations with them, or request that customer information be entered into a form.

Interactivity allows an online merchant to engage a consumer in ways similar to a face-to-face experience. Comment features, community forums, and social networks with social sharing functionality such as Like and Share buttons all enable consumers to actively interact with merchants and other users. Somewhat less obvious forms of interactivity include responsive design elements, such as websites that change format depending on what kind of device they are being viewed on, product images that change as a mouse hovers over them, the ability to zoom in or rotate images, forms that notify the user of a problem as they are being filled out, and search boxes that autofill as the user types.

INFORMATION DENSITY

information density
the total amount and quality of information available to all market participants

E-commerce technologies vastly increase **information density**—the total amount and quality of information available to all market participants, consumers and merchants alike. E-commerce technologies reduce information collection, storage, processing, and communication costs. At the same time, these technologies greatly increase the currency, accuracy, and timeliness of information—making information more useful and important than ever. As a result, information becomes more plentiful, less expensive, and of higher quality.

A number of business consequences result from the growth in information density. One of the shifts that e-commerce is bringing about is a reduction in information asymmetry among market participants (consumers and merchants). Prices and costs become more transparent. *Price transparency* refers to the ease with which consumers can find out the variety of prices in a market; *cost transparency* refers to the ability of consumers to discover the actual costs merchants pay for products. Preventing consumers from learning about prices and costs becomes more difficult with e-commerce and, as a result, the entire marketplace potentially becomes more price competitive (Sinha, 2000). But there are advantages for merchants as well. Online merchants can discover much more about consumers; this allows merchants to segment the market into groups willing to pay different prices and permits them to engage in *price discrimination*—selling the same goods, or nearly the same goods, to different targeted groups at different prices. For instance, an online merchant can discover a consumer's avid interest in expensive exotic vacations, and then pitch expensive exotic vacation plans to that consumer at a premium price, knowing this person is willing to pay extra for such a vacation. At the same time, the online merchant can pitch the same vacation plan at a lower price to more price-sensitive consumers. Merchants also have enhanced abilities to differentiate their products in terms of cost, brand, and quality.

PERSONALIZATION AND CUSTOMIZATION

E-commerce technologies permit **personalization**: merchants can target their marketing messages to specific individuals by adjusting the message to a person's name, interests, and past purchases. Today this is achieved in a few milliseconds and followed by an advertisement based on the consumer's profile. The technology also permits **customization**—changing the delivered product or service based on a user's preferences or prior behavior. Given the interactive nature of e-commerce technology, much information about the consumer can be gathered in the marketplace at the moment of purchase.

personalization
the targeting of marketing messages to specific individuals by adjusting the message to a person's name, interests, and past purchases

customization
changing the delivered product or service based on a user's preferences or prior behavior

With the increase in information density, a great deal of information about the consumer's past purchases and behavior can be stored and used by online merchants. The result is a level of personalization and customization unthinkable with traditional commerce technologies. For instance, you may be able to shape what you see on television by selecting a channel, but you cannot change the contents of the channel you have chosen. In contrast, the online version of the *Wall Street Journal* allows you to select the type of news stories you want to see first, and gives you the opportunity to be alerted when certain events happen. Personalization and customization allow firms to precisely identify market segments and adjust their messages accordingly.

SOCIAL TECHNOLOGY: USER-GENERATED CONTENT AND SOCIAL NETWORKS

In a way quite different from all previous technologies, e-commerce technologies have evolved to be much more social by allowing users to create and share content with a worldwide community. Using these forms of communication, users are able to create new social networks and strengthen existing ones.

All previous mass media in modern history, including the printing press, used a broadcast model (one-to-many): content is created in a central location by experts (professional writers, editors, directors, actors, and producers) and audiences are concentrated in huge aggregates to consume a standardized product. The telephone would appear to be an exception but it is not a mass communication technology. Instead the telephone is a one-to-one technology. E-commerce technologies have the potential to invert this standard media model by giving users the power to create and distribute content on a large scale, and permit users to program their own content consumption. E-commerce technologies provide a unique, many-to-many model of mass communication.

Table 1.2 provides a summary of each of the unique features of e-commerce technology and their business significance.

1.4 TYPES OF E-COMMERCE

There are a number of different types of e-commerce and many different ways to characterize them. For the most part, we distinguish different types of e-commerce

TABLE 1.2 BUSINESS SIGNIFICANCE OF THE EIGHT UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY

E-COMMERCE TECHNOLOGY DIMENSION	BUSINESS SIGNIFICANCE
Ubiquity—E-commerce technology is available everywhere: at work, at home, and elsewhere via mobile devices, anytime.	The marketplace is extended beyond traditional boundaries and is removed from a temporal and geographic location. "Marketspace" is created; shopping can take place anywhere. Customer convenience is enhanced, and shopping costs are reduced.
Global reach—The technology reaches across national boundaries, around the earth.	Commerce is enabled across cultural and national boundaries seamlessly and without modification. "Marketspace" includes potentially billions of consumers and millions of businesses worldwide.
Universal standards—There is one set of technology standards.	There is a common, inexpensive, global technology foundation for businesses to use.
Richness—Video, audio, and text messages are possible.	Video, audio, and text marketing messages are integrated into a single marketing message and consuming experience.
Interactivity—The technology works through interaction with the user.	Consumers are engaged in a dialog that dynamically adjusts the experience to the individual, and makes the consumer a co-participant in the process of delivering goods to the market.
Information density—The technology reduces information costs and raises quality.	Information processing, storage, and communication costs drop dramatically, while currency, accuracy, and timeliness improve greatly. Information becomes plentiful, cheap, and accurate.
Personalization/Customization—The technology allows personalized messages to be delivered to individuals as well as groups.	Personalization of marketing messages and customization of products and services are based on individual characteristics.
Social technology—User-generated content and social networks.	New online social and business models enable user content creation and distribution, and support social networks.

by the nature of the market relationship—who is selling to whom. Mobile, social, and local e-commerce can be looked at as subsets of these types of e-commerce.

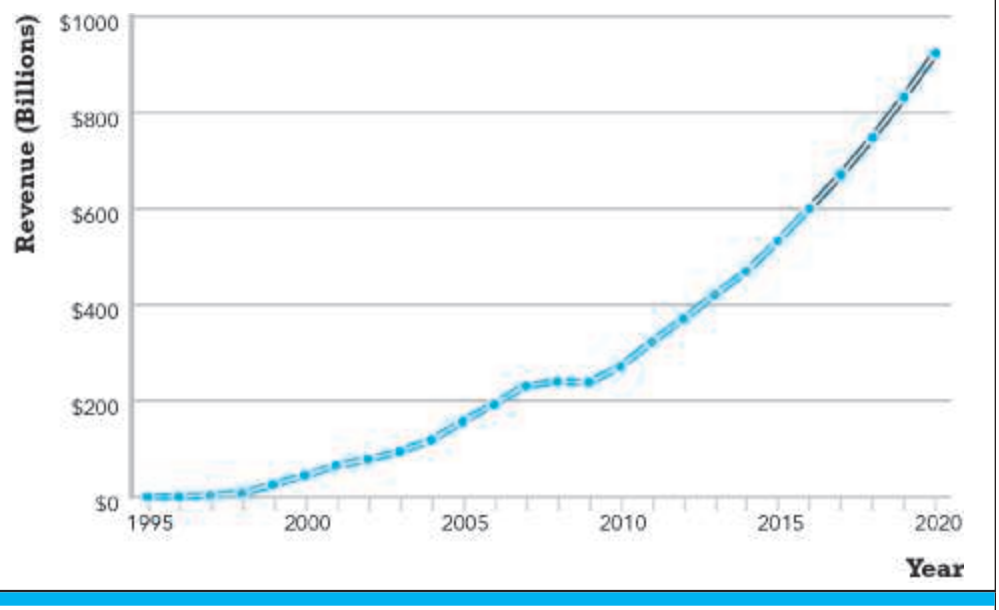
BUSINESS-TO-CONSUMER (B2C) E-COMMERCE

business-to-consumer (B2C) e-commerce
online businesses selling to individual consumers

The most commonly discussed type of e-commerce is **business-to-consumer (B2C) e-commerce**, in which online businesses attempt to reach individual consumers. B2C e-commerce includes purchases of retail goods, travel and other types of services, and online content. Even though B2C is comparatively small (an estimated $600 billion in 2016 in the United States), it has grown exponentially since 1995, and is the type of e-commerce that most consumers are likely to encounter (see **Figure 1.5**).

Within the B2C category, there are many different types of business models. Chapter 2 has a detailed discussion of seven different B2C business models: online

FIGURE 1.5 THE GROWTH OF B2C E-COMMERCE IN THE UNITED STATES



In the early years, B2C e-commerce was doubling or tripling each year. Although B2C e-commerce growth in the United States slowed in 2008–2009 due to the economic recession, it resumed growing at about 13% in 2010 and since then, has continued to grow at double-digit rates.

SOURCES: Based on data from eMarketer, Inc., 2016e, 2016f; authors' estimates.

retailers, service providers, transaction brokers, content providers, community providers/social networks, market creators, and portals. Then, in Part 4, we look at each of these business models in action. In Chapter 9, we examine online retailers, service providers, including on-demand services, and transaction brokers. In Chapter 10, we focus on content providers. In Chapter 11, we look at community providers (social networks), market creators (auctions), and portals.

The data suggests that, over the next five years, B2C e-commerce in the United States will grow by over 10% annually. There is tremendous upside potential. Today, for instance, retail e-commerce (which currently comprises the lion's share of B2C e-commerce revenues) is still a very small part (around 8%) of the overall $4.8 trillion retail market in the United States. There is obviously much room to grow (see **Figure 1.6**). However, it's not likely that B2C e-commerce revenues will continue to expand forever at current rates. As online sales become a larger percentage of all sales, online sales growth will likely eventually decline. However, this point still appears to be a long way off. Online content sales, everything from music, to video, medical information, games, and entertainment, have an even longer period to grow before they hit any ceiling effects.

BUSINESS-TO-BUSINESS (B2B) E-COMMERCE

business-to-business (B2B) e-commerce online businesses selling to other businesses

Business-to-business (B2B) e-commerce, in which businesses focus on selling to other businesses, is the largest form of e-commerce, with around $6.7 trillion in

FIGURE 1.6 ROOM TO GROW

The retail e-commerce market is still just a small part of the overall U.S. retail market, but with much room to grow in the future.

transactions in the United States in 2016 (see **Figure 1.7**). There is an estimated $14.5 trillion in business-to-business exchanges of all kinds, online and offline, suggesting that B2B e-commerce has significant growth potential. The ultimate size of B2B e-commerce is potentially huge.

There are two primary business models used within the B2B arena: Net marketplaces, which include e-distributors, e-procurement companies, exchanges and industry consortia, and private industrial networks. We review various B2B business models in Chapter 2 and examine them in further depth in Chapter 12.

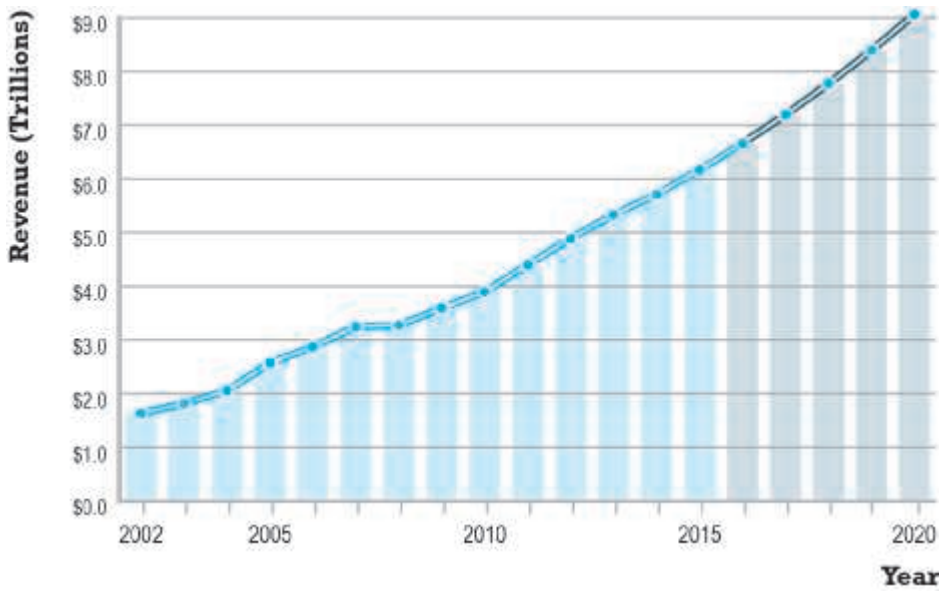
CONSUMER-TO-CONSUMER (C2C) E-COMMERCE

consumer-to-consumer (C2C) e-commerce
consumers selling to other consumers

Consumer-to-consumer (C2C) e-commerce provides a way for consumers to sell to each other, with the help of an online market maker (also called a platform provider) such as eBay or Etsy, the classifieds site Craigslist, or on-demand service companies such as Airbnb and Uber. In C2C e-commerce, the consumer prepares the product for market, places the product for auction or sale, and relies on the market maker to provide catalog, search engine, and transaction-clearing capabilities so that products can be easily displayed, discovered, and paid for.

Given that in 2015, eBay by itself generated around $82 billion in gross merchandise volume, it is probably safe to estimate that the size of the C2C market in 2016 is more than $100 billion (eBay, 2016).

FIGURE 1.7 THE GROWTH OF B2B E-COMMERCE IN THE UNITED STATES



B2B e-commerce in the United States is about 10 times the size of B2C e-commerce. In 2020, B2B e-commerce is projected to be over $9 trillion. (Note: Does not include EDI transactions.)

SOURCES: Based on data from U.S. Census Bureau, 2016; authors' estimates.

MOBILE E-COMMERCE (M-COMMERCE)

Mobile e-commerce (m-commerce), refers to the use of mobile devices to enable online transactions. M-commerce involves the use of cellular and wireless networks to connect smartphones and tablet computers to the Internet. Once connected, mobile consumers can purchase products and services, make travel reservations, use an expanding variety of financial services, access online content, and much more.

mobile e-commerce (m-commerce)
use of mobile devices to enable online transactions

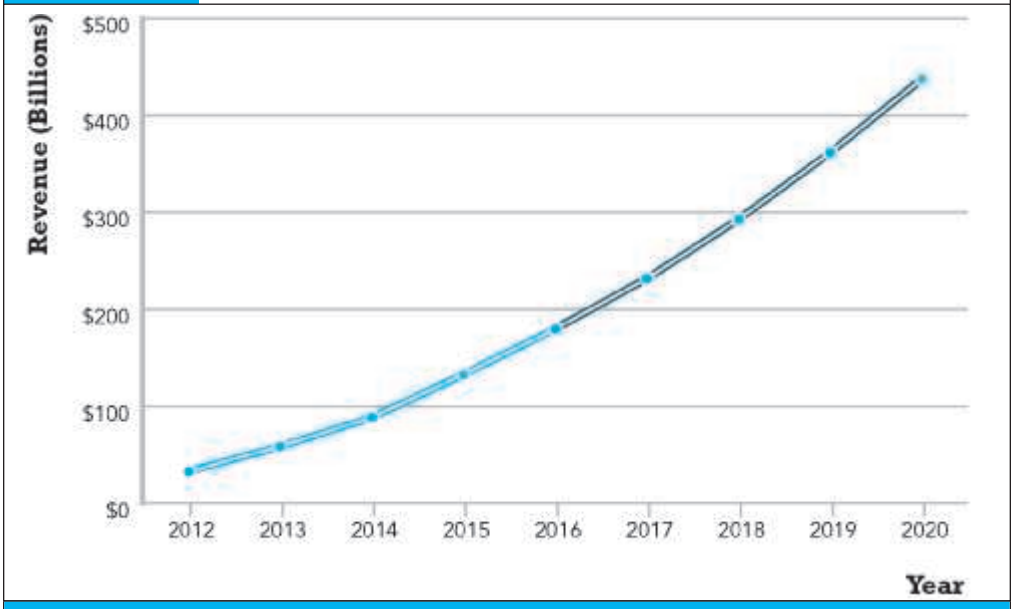
M-commerce purchases are expected to reach over $180 billion in 2016 and to grow rapidly in the United States over the next five years (see **Figure 1.8**). Factors that are driving the growth of m-commerce include the increasing amount of time consumers are spending using mobile devices, larger smartphone screen sizes, greater use of responsive design enabling e-commerce sites to be better optimized for mobile use and mobile checkout and payment, and enhanced mobile search functionality. (eMarketer, Inc., 2016g, 2016h).

SOCIAL E-COMMERCE

Social e-commerce is e-commerce that is enabled by social networks and online social relationships. The growth of social e-commerce is being driven by a number of factors, including the increasing popularity of social sign-on (signing onto websites using your Facebook or other social network ID), network notification (the sharing of approval or disapproval of products, services, and content), online collaborative

social e-commerce
e-commerce enabled by social networks and online social relationships

FIGURE 1.8 THE GROWTH OF M-COMMERCE IN THE UNITED STATES



In the last five years, m-commerce has increased astronomically, from just $32.8 billion in 2012 to over an expected $180 billion in 2016, and it is anticipated that it will continue to grow at double-digit rates over the next five years as consumers become more and more accustomed to using mobile devices to purchase products and services.

SOURCES: Based on data from eMarketer, Inc., 2016g, 2016h, 2015a, 2015b, 2014.

shopping tools, social search (recommendations from online trusted friends), and the increasing prevalence of integrated social commerce tools such as Buy buttons, Shopping tabs, and virtual shops on Facebook, Instagram, Pinterest, YouTube, and other social network sites.

Social e-commerce is still in its relative infancy, but in 2015, the top 500 retailers in Internet Retailer's Social Media 500 earned about $3.9 billion from social e-commerce. Website traffic from social networks to the top 500 retailers also increased by almost 20% in 2015 (Internet Retailer, 2016).

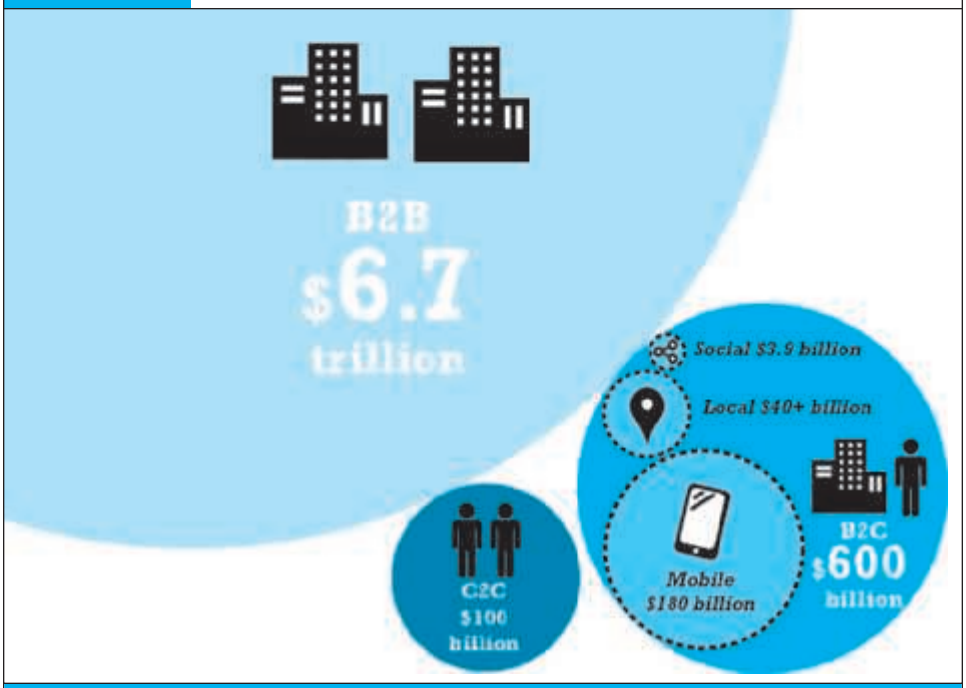
Social e-commerce is often intertwined with m-commerce, particularly as more and more social network users access those networks via mobile devices. A variation of social e-commerce known as *conversational commerce* leverages the mobile connection even further. Conversational commerce involves the use of mobile messaging apps such as Facebook Messenger, WhatsApp, Snapchat, Slack, and others as a vehicle for companies to engage with consumers.

local e-commerce
e-commerce that is focused on engaging the consumer based on his or her current geographic location

LOCAL E-COMMERCE

Local e-commerce, as its name suggests, is a form of e-commerce that is focused on engaging the consumer based on his or her current geographic location. Local merchants use a variety of online marketing techniques to drive consumers to their stores.

FIGURE 1.9 **THE RELATIVE SIZE OF DIFFERENT TYPES OF E-COMMERCE**



B2B e-commerce dwarfs all other forms of e-commerce; mobile, social, and local e-commerce, although growing rapidly, are still relatively small in comparison to "traditional" e-commerce.

Local e-commerce is the third prong of the mobile, social, local e-commerce wave and, fueled by an explosion of interest in local on-demand services such as Uber, is expected to grow in the United States to over $40 billion in 2016.

Figure 1.9 illustrates the relative size of all of the various types of e-commerce while **Table 1.3** provides examples for each type.

1.5 E-COMMERCE: A BRIEF HISTORY

It is difficult to pinpoint just when e-commerce began. There were several precursors to e-commerce. In the late 1970s, a pharmaceutical firm named Baxter Healthcare initiated a primitive form of B2B e-commerce by using a telephone-based modem that permitted hospitals to reorder supplies from Baxter. This system was later expanded during the 1980s into a PC-based remote order entry system and was widely copied throughout the United States long before the Internet became a commercial environment. The 1980s saw the development of Electronic Data Interchange (EDI) standards that permitted firms to exchange commercial documents and conduct digital commercial transactions across private networks.

TABLE 1.3 MAJOR TYPES OF E-COMMERCE

TYPE OF E-COMMERCE	EXAMPLE
B2C—business-to-consumer	Amazon is a general merchandiser that sells consumer products to retail consumers.
B2B—business-to-business	Go2Paper is an independent third-party marketplace that serves the paper industry.
C2C—consumer-to-consumer	Auction sites such as eBay, and listing sites such as Craigslist, enable consumers to auction or sell goods directly to other consumers. Airbnb and Uber provide similar platforms for services such as room rental and transportation.
M-commerce—mobile e-commerce	Mobile devices such as tablet computers and smartphones can be used to conduct commercial transactions.
Social e-commerce	Facebook is both the leading social network and social e-commerce site.
Local e-commerce	Groupon offers subscribers daily deals from local businesses in the form of Groupons, discount coupons that take effect once enough subscribers have agreed to purchase.

In the B2C arena, the first truly large-scale digitally enabled transaction system was the Minitel, a French videotext system that combined a telephone with an 8-inch screen. The Minitel was first introduced in 1981, and by the mid-1980s, more than 3 million had been deployed, with more than 13,000 different services available, including ticket agencies, travel services, retail products, and online banking. The Minitel service continued in existence until December 31, 2006, when it was finally discontinued by its owner, France Telecom.

However, none of these precursor systems had the functionality of the Internet. Generally, when we think of e-commerce today, it is inextricably linked to the Internet. For our purposes, we will say e-commerce begins in 1995, following the appearance of the first banner advertisements placed by AT&T, Volvo, Sprint, and others on Hotwired in late October 1994, and the first sales of banner ad space by Netscape and Infoseek in early 1995.

Although e-commerce is not very old, it already has a tumultuous history, which can be usefully divided into three periods: 1995–2000, the period of invention; 2001–2006, the period of consolidation; and 2007–present, a period of reinvention with social, mobile, and local expansion. The following examines each of these periods briefly, while **Figure 1.10** places them in context along a timeline.

E-COMMERCE 1995–2000: INVENTION

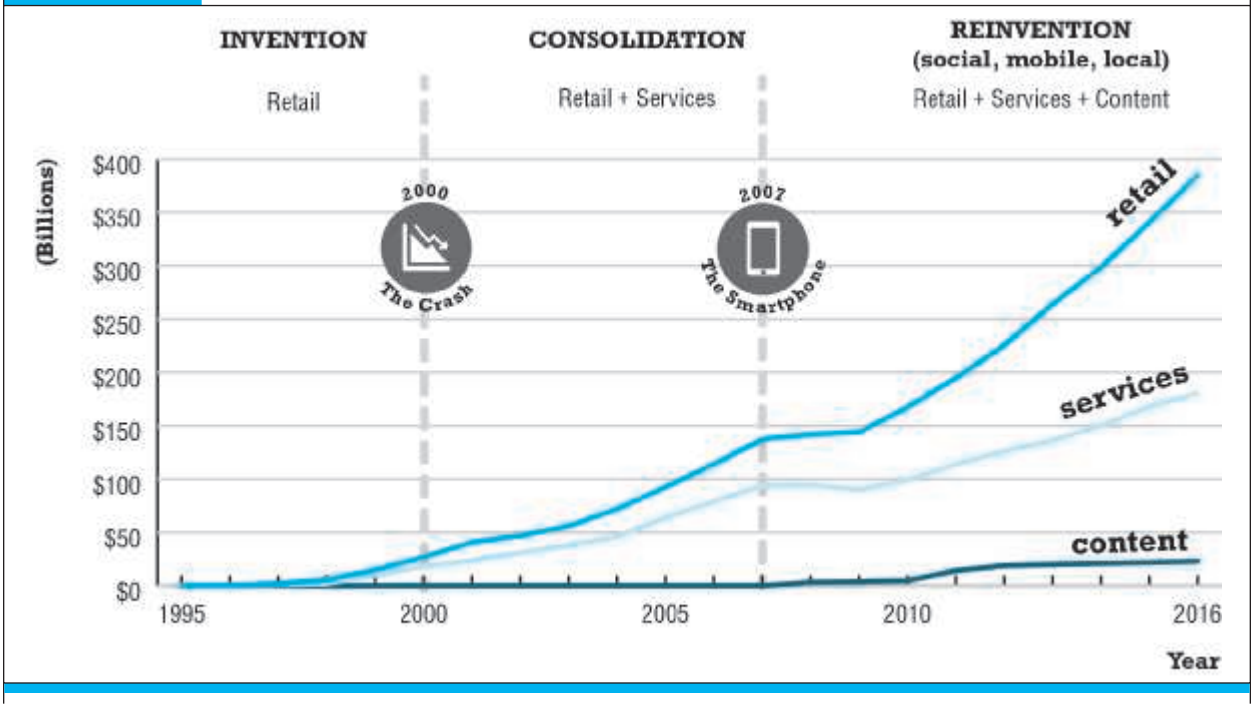
The early years of e-commerce were a period of explosive growth and extraordinary innovation. During this Invention period, e-commerce meant selling retail goods, usually quite simple goods, on the Internet. There simply was not enough bandwidth for more complex products. Marketing was limited to unsophisticated static display ads and not very powerful search engines. The web policy of most large firms, if they had one at all, was to have a basic static website depicting their brands. The rapid

growth in e-commerce was fueled by over $125 billion in venture capital. This period of e-commerce came to a close in 2000 when stock market valuations plunged, with thousands of companies disappearing (the "dot-com crash").

The early years of e-commerce were also one of the most euphoric of times in American commercial history. It was also a time when key e-commerce concepts were developed. For computer scientists and information technologists, the early success of e-commerce was a powerful vindication of a set of information technologies that had developed over a period of 40 years—extending from the development of the early Internet, to the PC, to local area networks. The vision was of a universal communications and computing environment that everyone on Earth could access with cheap, inexpensive computers—a worldwide universe of knowledge stored on HTML pages created by hundreds of millions of individuals and thousands of libraries, governments, and scientific institutes. Technologists celebrated the fact that the Internet was not controlled by anyone or any nation, but was free to all. They believed the Internet—and the e-commerce that rose on this infrastructure—should remain a self-governed, self-regulated environment.

For economists, the early years of e-commerce raised the realistic prospect of a nearly perfect competitive market: where price, cost, and quality information are equally distributed, a nearly infinite set of suppliers compete against one another, and customers have access to all relevant market information worldwide. The Internet would spawn digital markets where information would be nearly perfect—something that is rarely true in other real-world markets. Merchants in turn would have equal

FIGURE 1.10 **PERIODS IN THE DEVELOPMENT OF E-COMMERCE**



direct access to hundreds of millions of customers. In this near-perfect information marketspace, transaction costs would plummet because search costs—the cost of searching for prices, product descriptions, payment settlement, and order fulfillment—would all fall drastically (Bakos, 1997). For merchants, the cost of searching for customers would also fall, reducing the need for wasteful advertising. At the same time, advertisements could be personalized to the needs of every customer. Prices and even costs would be increasingly transparent to the consumer, who could now know exactly and instantly the worldwide best price, quality, and availability of most products. Information asymmetry would be greatly reduced. Given the instant nature of Internet communications, the availability of powerful sales information systems, and the low cost involved in changing prices on a website (low menu costs), producers could dynamically price their products to reflect actual demand, ending the idea of one national price, or one suggested manufacturer's list price. In turn, market middlemen—the distributors and wholesalers who are intermediaries between producers and consumers, each demanding a payment and raising costs while adding little value—would disappear (**disintermediation**). Manufacturers and content originators would develop direct market relationships with their customers. The resulting intense competition, the decline of intermediaries, and the lower transaction costs would eliminate product brands, and along with these, the possibility of *monopoly profits* based on brands, geography, or special access to factors of production. Prices for products and services would fall to the point where prices covered costs of production plus a fair, "market rate" of return on capital, plus additional small payments for entrepreneurial effort (that would not last long). Unfair competitive advantages (which occur when one competitor has an advantage others cannot purchase) would be reduced, as would extraordinary returns on invested capital. This vision was called **friction-free commerce** (Smith et al., 2000).

disintermediation
displacement of market middlemen who traditionally are intermediaries between producers and consumers by a new direct relationship between producers and consumers

friction-free commerce
a vision of commerce in which information is equally distributed, transaction costs are low, prices can be dynamically adjusted to reflect actual demand, intermediaries decline, and unfair competitive advantages are eliminated

first mover
a firm that is first to market in a particular area and that moves quickly to gather market share

For real-world entrepreneurs, their financial backers, and marketing professionals, e-commerce represented an extraordinary opportunity to earn far above normal returns on investment. This is just the opposite of what economists hoped for. The e-commerce marketspace represented access to millions of consumers worldwide who used the Internet and a set of marketing communications technologies (e-mail and web pages) that was universal, inexpensive, and powerful. These new technologies would permit marketers to practice what they always had done—segmenting the market into groups with different needs and price sensitivity, targeting the segments with branding and promotional messages, and positioning the product and pricing for each group—but with even more precision. In this new marketspace, extraordinary profits would go to **first movers**—those firms who were first to market in a particular area and who moved quickly to gather market share. In a "winner take all" market, first movers could establish a large customer base quickly, build brand name recognition early, create an entirely new distribution channel, and then inhibit competitors (new entrants) by building in *switching costs* for their customers through proprietary interface designs and features available only at one site. The idea for entrepreneurs was to create near monopolies online based on size, convenience, selection, and brand. Online businesses using the new technology could create informative, community-like features unavailable to traditional merchants. These "communities of consumption"

also would add value and be difficult for traditional merchants to imitate. The thinking was that once customers became accustomed to using a company's unique web interface and feature set, they could not easily be switched to competitors. In the best case, the entrepreneurial firm would invent proprietary technologies and techniques that almost everyone adopted, creating a network effect. A **network effect** occurs where all participants receive value from the fact that everyone else uses the same tool or product (for example, a common operating system, telephone system, or software application such as a proprietary instant messaging standard or an operating system such as Windows), all of which increase in value as more people adopt them.[1]

network effect
occurs where users receive value from the fact that everyone else uses the same tool or product

To initiate this process, entrepreneurs argued that prices would have to be very low to attract customers and fend off potential competitors. E-commerce was, after all, a totally new way of shopping that would have to offer some immediate cost benefits to consumers. However, because doing business on the Web was supposedly so much more efficient when compared to traditional "bricks-and-mortar" businesses (even when compared to the direct mail catalog business) and because the costs of customer acquisition and retention would supposedly be so much lower, profits would inevitably materialize out of these efficiencies. Given these dynamics, market share, the number of visitors to a site ("eyeballs"), and gross revenue became far more important in the earlier stages of an online firm than earnings or profits. Entrepreneurs and their financial backers in the early years of e-commerce expected that extraordinary profitability would come, but only after several years of losses.

Thus, the early years of e-commerce were driven largely by visions of profiting from new technology, with the emphasis on quickly achieving very high market visibility. The source of financing was venture capital funds. The ideology of the period emphasized the ungoverned "Wild West" character of the Web and the feeling that governments and courts could not possibly limit or regulate the Internet; there was a general belief that traditional corporations were too slow and bureaucratic, too stuck in the old ways of doing business, to "get it"—to be competitive in e-commerce. Young entrepreneurs were therefore the driving force behind e-commerce, backed by huge amounts of money invested by venture capitalists. The emphasis was on *disrupting* (destroying) traditional distribution channels and disintermediating existing channels, using new pure online companies who aimed to achieve impregnable first-mover advantages. Overall, this period of e-commerce was characterized by experimentation, capitalization, and hypercompetition (Varian, 2000b).

E-COMMERCE 2001–2006: CONSOLIDATION

In the second period of e-commerce, from 2000 to 2006, a sobering period of reassessment of e-commerce occurred, with many critics doubting its long-term prospects. Emphasis shifted to a more "business-driven" approach rather than being technology driven; large traditional firms learned how to use the Web to strengthen their market positions; brand extension and strengthening became more important than creating

[1] The network effect is quantified by Metcalfe's Law, which argues that the value of a network grows by the square of the number of participants.

new brands; financing shrunk as capital markets shunned startup firms; and traditional bank financing based on profitability returned.

During this period of consolidation, e-commerce changed to include not just retail products but also more complex services such as travel and financial services. This period was enabled by widespread adoption of broadband networks in American homes and businesses, coupled with the growing power and lower prices of personal computers that were the primary means of accessing the Internet, usually from work or home. Marketing on the Internet increasingly meant using search engine advertising targeted to user queries, rich media and video ads, and behavioral targeting of marketing messages based on ad networks and auction markets. The web policy of both large and small firms expanded to include a broader "web presence" that included not just websites, but also e-mail, display, and search engine campaigns; multiple websites for each product; and the building of some limited community feedback facilities. E-commerce in this period was growing again by more than 10% a year.

E-COMMERCE 2007–PRESENT: REINVENTION

Web 2.0
set of applications and technologies that enable user-generated content

Beginning in 2007 with the introduction of the iPhone, to the present day, e-commerce has been transformed yet again by the rapid growth of **Web 2.0** (a set of applications and technologies that enable user-generated content, such as online social networks, blogs, video and photo sharing sites, and wikis), widespread adoption of mobile devices such as smartphones and tablet computers, the expansion of e-commerce to include local goods and services, and the emergence of an on-demand service economy enabled by millions of apps on mobile devices and cloud computing. This period can be seen as both a sociological, as well as a technological and business, phenomenon.

The defining characteristics of this period are often characterized as the "social, mobile, local" online world. Entertainment content has developed as a major source of e-commerce revenues and mobile devices have become entertainment centers, as well as on-the-go shopping devices for retail goods and services. Marketing has been transformed by the increasing use of social networks, word-of-mouth, viral marketing, and much more powerful data repositories and analytic tools for truly personal marketing. Firms have greatly expanded their online presence by moving beyond static web pages to social networks such as Facebook, Twitter, Pinterest, and Instagram in an attempt to surround the online consumer with coordinated marketing messages. These social networks share many common characteristics. First, they rely on user-generated content. "Regular" people (not just experts or professionals) are creating, sharing, and broadcasting content to huge audiences. They are inherently highly interactive, creating new opportunities for people to socially connect to others. They attract extremely large audiences (about 1.7 billion monthly active users worldwide as of June 2016 in the case of Facebook). These audiences present marketers with extraordinary opportunities for targeted marketing and advertising.

More recently, the reinvention of e-commerce has resulted in a new set of on-demand, personal service businesses such as Uber, Airbnb, Instacart, and Handy. These businesses have been able to tap into a large reservoir of unused assets (cars, spare rooms, and personal spare time) and to create lucrative markets based on the mobile platform infrastructure. The *Insight on Business* case, *Startup Boot Camp,* takes

a look at Y Combinator, which has mentored a number of these new social, mobile, and local e-commerce ventures.

Table 1.4 summarizes e-commerce in each of these three periods.

ASSESSING E-COMMERCE: SUCCESSES, SURPRISES, AND FAILURES

Looking back at the evolution of e-commerce, it is apparent that e-commerce has been a stunning technological success as the Internet and the Web ramped up from a few thousand to billions of e-commerce transactions per year, and this year will generate an estimated $600 billion in total B2C revenues and around $6.7 trillion in B2B revenues, with around 177 million online buyers in the United States. With enhancements and strengthening, described in later chapters, it is clear that e-commerce's digital infrastructure is solid enough to sustain significant growth in e-commerce during the next decade. The Internet scales well. The "e" in e-commerce has been an overwhelming success.

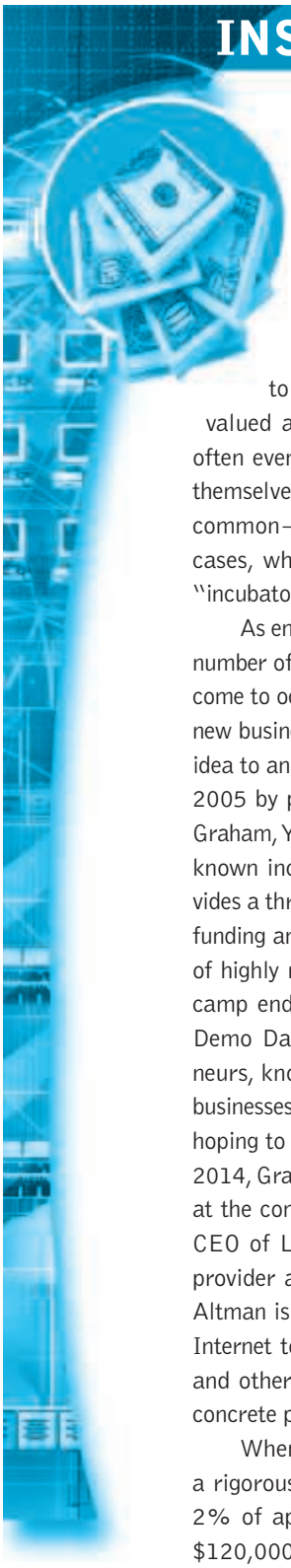
From a business perspective, though, the early years of e-commerce were a mixed success, and offered many surprises. Only a very small percentage of dot-coms formed

TABLE 1.4 EVOLUTION OF E-COMMERCE

1995–2000 INVENTION	2001–2006 CONSOLIDATION	2007–PRESENT REINVENTION
Technology driven	Business driven	Mobile technology enables social, local, and mobile e-commerce
Revenue growth emphasis	Earnings and profits emphasis	Audience and social network connections emphasis
Venture capital financing	Traditional financing	Return of venture capital financing; buy-outs of startups by large firms
Ungoverned	Stronger regulation and governance	Extensive government surveillance
Entrepreneurial	Large traditional firms	Entrepreneurial social, mobile, and local firms
Disintermediation	Strengthening intermediaries	Proliferation of small online intermediaries renting business processes of larger firms
Perfect markets	Imperfect markets, brands, and network effects	Continuation of online market imperfections; commodity competition in select markets
Pure online strategies	Mixed "bricks-and-clicks" strategies	Return of pure online strategies in new markets; extension of bricks-and-clicks in traditional retail markets
First-mover advantages	Strategic-follower strength; complementary assets	First-mover advantages return in new markets as traditional web players catch up
Low-complexity retail products	High-complexity retail products and services	Retail, services, and content

INSIGHT ON BUSINESS

STARTUP BOOT CAMP



By now we've all heard the story of some lines of code written by Mark Zuckerberg in a Harvard dorm room blossoming into a multi-billion dollar business. These days, it's harder than ever to keep track of all the tech start-ups being valued at millions and even billions of dollars, often even without a cent of revenue to show for themselves. A number of them have something in common—they have been nurtured, and in some cases, whipped into shape, with the help of an "incubator."

As entrepreneurs continue to launch a growing number of e-commerce companies, incubators have come to occupy a vital role in Silicon Valley, helping new businesses move from little more than a great idea to an established, vibrant business. Founded in 2005 by programmer and venture capitalist Paul Graham, Y Combinator (YC) is Silicon Valley's best known incubator. Twice a year the company provides a three-month boot camp, complete with seed funding and mentorship from an extensive network of highly regarded tech entrepreneurs. Every boot camp ends with a demonstration day, known as Demo Day or D Day, where all of the entrepreneurs, known as "founders," pitch their fledgling businesses to a group of wealthy venture capitalists hoping to unearth the next Facebook or Google. In 2014, Graham stepped down from a leadership role at the company, replaced by Sam Altman, former CEO of Loopt, a location-based mobile services provider and a successful YC graduate company. Altman is aiming to expand YC's focus beyond the Internet to energy, biotechnology, medical devices, and other "hard technology" startups that solve concrete problems.

When companies are admitted to YC after a rigorous selection progress (typically less than 2% of applicants are accepted), they are given $120,000 in cash in exchange for a 7% stake in the company. Founders have regular meetings with YC partners, and have free access to technology, technical advice, emotional support, and lessons in salesmanship. As of September 2016, Y Combinator has helped launch almost 1,400 start-up companies, which together have a market capitalization of more than $70 billion. Its graduates have raised more than $10 billion, and ten of them have attained once rare, but now increasingly common, "unicorn" status, with a valuation in excess of $1 billion. More than 50 are worth over $100 million.

YC has been so successful that it is sometimes referred to as a "unicorn breeder." Graduates that have achieved unicorn status include Airbnb, an on-demand room rental service (with a valuation of $30 billion); Dropbox, a cloud-based file storage service ($10 billion); Stripe, a digital payment infrastructure company ($5 billion); MZ (Machine Zone), a massively multi-player online gaming company ($3 billion); Zenefits, a cloud-based employee benefits manager ($2 billion); Instacart, an on-demand grocery delivery service ($2 billion); Twitch, a streaming video game network (acquired by Amazon for $1 billion); Docker, an open source software company ($1 billion), and Cruise, which develops self-driving car technology (acquired by GM for $ 1 billion). Other well-known graduates include Reddit, a social news site; Weebly, a website building platform; Coinbase, a Bitcoin wallet; Scribd, a digital library subscription service; and Codecademy, an online education service that teaches people how to program.

YC's Winter 2016 class featured 127 startups that launched during its March 2016 Demo Days. While YC is increasingly focused on startups that are aiming to solve pervasive problems in the world rather than the next big gaming or to-do list app, it still accepts a number of startups seeking to make their mark in the e-commerce arena. For instance, Restocks is a mobile app that helps consumers

track and buy hard-to-find, limited release products. Subscribers to Restocks' service receive push notification when brands such as Nike release or restock those products. Restocks had its genesis in founder Luke Miles' frustration with his inability to find and purchase some "hot" Supreme-brand t-shirts. Miles wrote some code that sent him an e-mail when the products showed up as restocked on the brand's website and then realized that it could be a useful tool for other products as well. Although Restocks faces competition from individual brands that may offer apps with a similar functionality, such as Nike's SNKRs app, Restocks differentiates itself by aggregating dozens of brands.

Among other startups from the Winter 2016 class tabbed by analysts as particularly promising were Cover (an app that enables users to obtain insurance just by taking a photo), Castle.io (behavior-based online security), Yardbook (a cloud software system for the landscaping industry), Mux (a Netflix-like streaming service for business looking to deliver online video to customers), and Chatfuel (an automated chat tool for WhatsApp and other platforms).

YC also accepts startups that are focused on markets outside the United States. The Winter 2016 class included Paystack, an online payments provider for African businesses; Kisan Network, which provides an online marketplace in India for farmers to sell directly to institutional buyers; Rappi, an on-demand service company focused on grocery delivery in Colombia; Shypmate, which offers a platform to facilitate person-to-person shipping to Africa; Lynks, an e-commerce logistics infrastructure company for countries that are less developed; and GoLorry, a mobile app that provides trucking logistics in India.

Not every company that makes it through YC's boot camp is successful. Companies that fail to attract sufficient investor interest at Demo Day can try again with a different company or go their own way and "grow organically." Some skeptics believe that incubators like YC might not be the best idea for every startup. For startups with solid, but not eye-popping products, services, or growth metrics, YC's D Day might actually hurt their chances of getting funding. Having to compete against an extremely qualified field of startup companies diminishes the appeal for less flashy businesses. Once you've failed at acquiring funding at YC, other prospective investors might become concerned. There is also the concern founders may fixate on raising more money in seed funding rounds than necessary. According to Altman, founders should initially focus on making their company work on as little capital as possible, and YC's best companies have been able to make great strides even with just relatively small amounts of seed funding.

As part of its own continuing evolution, YC announced in 2015 that it would begin to make later-stage investments in its graduates as well. Together with Stanford University's endowment fund and Willett Advisors, YC has created a new $700 million Continuity Fund. YC has said that it hopes to participate in later funding rounds for all of its graduates that are being valued in funding at $300 million or less to help further guide them as they mature. In 2016, background screening software maker Checkr was one of the first to benefit, raising $40 million in funding led by the Continuity Fund.

SOURCES: "Press," Y.combinator.com/press, accessed November 11, 2016; "Get Hype Brands at Retail with Restocks," by Matthew Panzarino, Techcrunch.com, April 19, 2016; "Inside Silicon Valley's Big Pitch Day," by Anna Wiener, *The Atlantic,* March 29, 2016; "4 Cloud Startups to Watch from Y Combinator," by Tess Townsend, Inc.com, March 24, 2016; "The Top 8 Startups from Y Combinator Winter '16 Demo Day 2," by Josh Constine, Techcrunch.com, March 24, 2016; "The Top 7 Startups From Y Combinator Winter '16 Demo Day 1," by Josh Constine, Techcrunch.com, March 23, 2016; "Checkr Raises $40 Million Series B Led by Y Combinator Continuity Fund," Ivp.com, March 23, 2016; "Stanford, Michael Bloomberg Now Back Every Y Combinator Startup," by Douglas Macmillan, *Wall Street Journal,* October 15, 2015; "Y Combinator Will Fund Later-Stage Companies," by Mike Isaac, *New York Times,* October 15, 2015; "Meet Y Combinator's Bold Whiz Kid Boss," by Jason Ankeny, Entrepreneur.com, April 25, 2015; "The Y Combinator Chronicles: Y Combinator President Sam Altman Is Dreaming Big," by Max Chafkin, Fastcompany.com, April 16, 2015; "Y Combinator Known for Picking Winners," by Heather Somerville, *San Jose Mercury News,* May 8, 2014; "Y Combinator's New Deal for Startups: More Money, Same 7% Equity," by Kia Kokalitcheva, Venturebeat.com, April 22, 2014; "The New Deal," by Sam Altman, Blog.ycombinator.com, April 22, 2014; "Silicon Valley's Start-up Machine," by Nathaniel Rich, *New York Times,* May 2, 2013; "What's the Secret Behind Y Combinator's Success?," by Drew Hansen, Forbes.com, February 18, 2013.

since 1995 have survived as independent companies in 2016, and even fewer of these survivors are profitable. Yet online retail sales of goods and services are still growing very rapidly. Contrary to economists' hopes, however, online sales are increasingly concentrated. For instance, according to Internet Retailer, the top 500 retailers account for 84% of all online retail sales (Internet Retailer, 2016). So thousands of firms have failed, and those few that have survived dominate the market. The idea of thousands of suppliers competing on price has been replaced by a market dominated by giant firms. Consumers use the Web as a powerful source of information about products they often actually purchase through other channels, such as at a traditional bricks-and-mortar store. For instance, a 2014 study found that almost 90% of those surveyed "webroomed" (researched a product online before purchasing at a physical store) (Interactions Consumer Experience Marketing, Inc., 2014). This is especially true of expensive consumer durables such as automobiles, appliances, and electronics. This offline "Internet-influenced" commerce is very difficult to estimate, but definitely significant. For instance, Forrester Research estimated the amount to be somewhere around $1.3 trillion in 2015 (Forrester Research, 2016). All together then, retail e-commerce (actual online purchases) and purchases influenced by online shopping but actually bought in a store (Internet-influenced commerce) are expected to amount to almost $1.7 trillion in 2016. The "commerce" in e-commerce is basically very sound, at least in the sense of attracting a growing number of customers and generating revenues and profits for large e-commerce players.

Although e-commerce has grown at an extremely rapid pace in customers and revenues, it is clear that many of the visions, predictions, and assertions about e-commerce developed in the early years have not been fulfilled. For instance, economists' visions of "friction-free" commerce have not been entirely realized. Prices are sometimes lower online, but the low prices are sometimes a function of entrepreneurs selling products below their costs. In some cases, online prices are higher than those of local merchants, as consumers are willing to pay a small premium for the convenience of buying online (Cavallo, 2016). Consumers are less price sensitive than expected; surprisingly, the websites with the highest revenue often have the highest prices. There remains considerable persistent and even increasing price dispersion: online competition has lowered prices, but price dispersion remains pervasive in many markets despite lower search costs (Levin, 2011; Ghose and Yao, 2010). In a study of 50,000 goods in the United Kingdom and the United States, researchers found Internet prices were sticky even in the face of large changes in demand, online merchants did not alter prices significantly more than offline merchants, and price dispersion across online sellers was somewhat greater than traditional brick and mortar stores (Gorodnichenko, et al., 2014). The concept of one world, one market, one price has not occurred in reality as entrepreneurs discover new ways to differentiate their products and services. Merchants have adjusted to the competitive Internet environment by engaging in "hit-and-run pricing" or changing prices every day or hour (using "flash pricing" or "flash sales") so competitors never know what they are charging (neither do customers); by making their prices hard to discover and sowing confusion among consumers by "baiting and switching" customers from low-margin products to high-margin products with supposedly "higher quality." Finally, brands remain very important in

e-commerce—consumers trust some firms more than others to deliver a high-quality product on time and they are willing to pay for it (Rosso and Jansen, 2010).

The "perfect competition" model of extreme market efficiency has not come to pass. Merchants and marketers are continually introducing information asymmetries. Search costs have fallen overall, but the overall transaction cost of actually completing a purchase in e-commerce remains high because users have a bewildering number of new questions to consider: Will the merchant actually deliver? What is the time frame of delivery? Does the merchant really stock this item? How do I fill out this form? Many potential e-commerce purchases are terminated in the shopping cart stage because of these consumer uncertainties. Some people still find it easier to call a trusted catalog merchant on the telephone than to order on a website. Finally, intermediaries have not disappeared as predicted. Most manufacturers, for instance, have not adopted the manufacturer-direct sales model of online sales, and some that had, such as Sony, have returned to an intermediary model. Dell, one of the pioneers of online manufacturer-direct sales, has moved toward a mixed model heavily reliant on in-store sales where customers can "kick the tires;" Apple's physical stores are among the most successful stores in the world. People still like to shop in a physical store.

If anything, e-commerce has created many opportunities for middlemen to aggregate content, products, and services and thereby introduce themselves as the "new" intermediaries. Third-party travel sites such as Travelocity, Orbitz, and Expedia are an example of this kind of intermediary. E-commerce has not driven existing retail chains and catalog merchants out of business, although it has created opportunities for entrepreneurial online-only firms to succeed.

The visions of many entrepreneurs and venture capitalists for e-commerce have not materialized exactly as predicted either. First-mover advantage appears to have succeeded only for a very small group of companies, albeit some of them extremely well-known, such as Google, Facebook, Amazon, and others. Getting big fast sometimes works, but often not. Historically, first movers have been long-term losers, with the early-to-market innovators usually being displaced by established "fast-follower" firms with the right complement of financial, marketing, legal, and production assets needed to develop mature markets, and this has proved true for e-commerce as well. Many e-commerce first movers, such as eToys, FogDog (sporting goods), Webvan (groceries), and Eve.com (beauty products), failed. Customer acquisition and retention costs during the early years of e-commerce were extraordinarily high, with some firms, such as E*Trade and other financial service firms, paying up to $400 to acquire a new customer. The overall costs of doing business online—including the costs of technology, site design and maintenance, and warehouses for fulfillment—are often no lower than the costs faced by the most efficient bricks-and-mortar stores. A large warehouse costs tens of millions of dollars regardless of a firm's online presence. The knowledge of how to run the warehouse is priceless, and not easily moved. The startup costs can be staggering. Attempting to achieve or enhance profitability by raising prices has often led to large customer defections. From the e-commerce merchant's perspective, the "e" in e-commerce does not stand for "easy."

On the other hand, there have been some extraordinary and unanticipated surprises in the evolution of e-commerce. Few predicted the impact of the mobile

platform. Few anticipated the rapid growth of social networks or their growing success as advertising platforms based on a more detailed understanding of personal behavior than even Google has achieved. And few, if any, anticipated the emergence of on-demand e-commerce, which enables people to use their mobile devices to order up everything from taxis, to groceries, to laundry service.

1.6 UNDERSTANDING E-COMMERCE: ORGANIZING THEMES

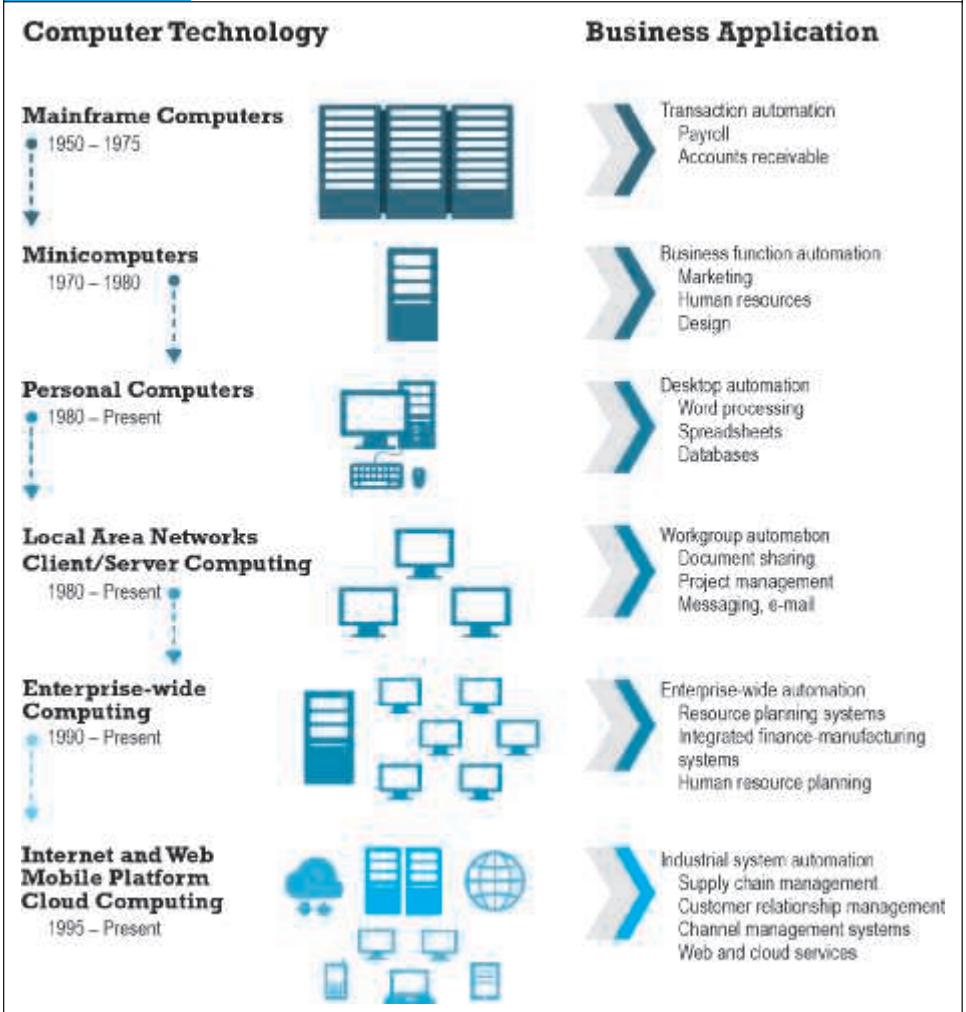
Understanding e-commerce in its totality is a difficult task for students and instructors because there are so many facets to the phenomenon. No single academic discipline is prepared to encompass all of e-commerce. After teaching the e-commerce course for a number of years and writing this book, we have come to realize just how difficult it is to "understand" e-commerce. We have found it useful to think about e-commerce as involving three broad interrelated themes: technology, business, and society. We do not mean to imply any ordering of importance here because this book and our thinking freely range over these themes as appropriate to the problem we are trying to understand and describe. Nevertheless, as in previous technologically driven commercial revolutions, there is a historic progression. Technologies develop first, and then those developments are exploited commercially. Once commercial exploitation of the technology becomes widespread, a host of social, cultural, and political issues arise, and society is forced to respond to them.

TECHNOLOGY: INFRASTRUCTURE

The development and mastery of digital computing and communications technology is at the heart of the newly emerging global digital economy we call e-commerce. To understand the likely future of e-commerce, you need a basic understanding of the information technologies upon which it is built. E-commerce is above all else a technologically driven phenomenon that relies on a host of information technologies as well as fundamental concepts from computer science developed over a 50-year period. At the core of e-commerce are the Internet and the Web, which we describe in detail in Chapter 3. Underlying these technologies are a host of complementary technologies: cloud computing, desktop computers, smartphones, tablet computers, local area networks, relational and non-relational databases, client/server computing, data mining, and fiber-optic switches, to name just a few. These technologies lie at the heart of sophisticated business computing applications such as enterprise-wide information systems, supply chain management systems, manufacturing resource planning systems, and customer relationship management systems. E-commerce relies on all these basic technologies—not just the Internet. The Internet, while representing a sharp break from prior corporate computing and communications technologies, is nevertheless just the latest development in the evolution of corporate computing and part of the continuing chain of computer-based innovations in business. **Figure 1.11** illustrates the major stages in the development of corporate computing and indicates how the Internet and the Web fit into this development trajectory.

To truly understand e-commerce, you will need to know something about packet-switched communications, protocols such as TCP/IP, client/server and cloud computing, mobile digital platforms, web servers, HTML5, CSS, and software programming tools such as Flash and JavaScript on the client side, and Java, PHP, Ruby on Rails, and ColdFusion on the server side. All of these topics are described fully in Part 2 of the book (Chapters 3–5).

FIGURE 1.11 THE INTERNET AND THE EVOLUTION OF CORPORATE COMPUTING



The Internet and Web, and the emergence of a mobile platform held together by the Internet cloud, are the latest in a chain of evolving technologies and related business applications, each of which builds on its predecessors.

THE INTERNET: KEY TECHNOLOGY CONCEPTS

In 1995, the Federal Networking Council (FNC) passed a resolution formally defining the term *Internet* as a network that uses the IP addressing scheme, supports the Transmission Control Protocol (TCP), and makes services available to users much like a telephone system makes voice and data services available to the public (see **Figure 3.2**).

Behind this formal definition are three extremely important concepts that are the basis for understanding the Internet: packet switching, the TCP/IP communications protocol, and client/server computing. Although the Internet has evolved and changed dramatically in the last 35 years, these three concepts are at the core of the way the Internet functions today and are the foundation for the Internet of the future.

packet switching
a method of slicing digital messages into packets, sending the packets along different communication paths as they become available, and then reassembling the packets once they arrive at their destination

packets
the discrete units into which digital messages are sliced for transmission over the Internet

Packet Switching

Packet switching is a method of slicing digital messages into discrete units called **packets**, sending the packets along different communication paths as they become available, and then reassembling the packets once they arrive at their destination (see **Figure 3.3**). Prior to the development of packet switching, early computer networks used leased, dedicated telephone circuits to communicate with terminals and other computers. In circuit-switched networks such as the telephone system, a complete point-to-point circuit is put together, and then communication can proceed. However, these "dedicated" circuit-switching techniques were expensive and wasted available communications capacity—the circuit would be maintained regardless of whether any data was being sent. For nearly 70% of the time, a dedicated voice circuit is not being fully used because of pauses between words and delays in assembling the circuit

FIGURE 3.2 RESOLUTION OF THE FEDERAL NETWORKING COUNCIL

"The Federal Networking Council (FNC) agrees that the following language reflects our definition of the term 'Internet.'

'Internet' refers to the global information system that—

(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;

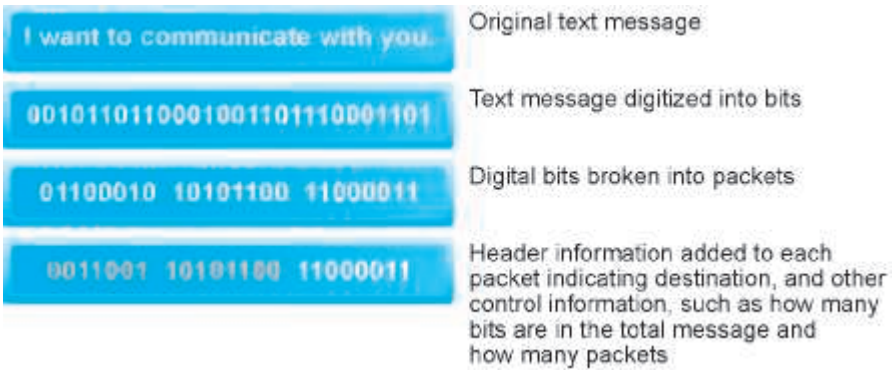
(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and

(iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein."

Last modified on October 30, 1995.

SOURCE: Federal Networking Council, 1995

FIGURE 3.3 PACKET SWITCHING



In packet switching, digital messages are divided into fixed-length packets of bits (generally about 1,500 bytes). Header information indicates both the origin and the ultimate destination address of the packet, the size of the message, and the number of packets the receiving node should expect. Because the receipt of each packet is acknowledged by the receiving computer, for a considerable amount of time, the network is not passing information, only acknowledgments, producing a delay called latency.

segments, both of which increase the length of time required to find and connect circuits. A better technology was needed.

The first book on packet switching was written by Leonard Kleinrock in 1964 (Kleinrock, 1964), and the technique was further developed by others in the defense research labs of both the United States and England. With packet switching, the communications capacity of a network can be increased by a factor of 100 or more. (The communications capacity of a digital network is measured in terms of bits per second.[2]) Imagine if the gas mileage of your car went from 15 miles per gallon to 1,500 miles per gallon—all without changing too much of the car!

In packet-switched networks, messages are first broken down into packets. Appended to each packet are digital codes that indicate a source address (the origination point) and a destination address, as well as sequencing information and error-control information for the packet. Rather than being sent directly to the destination address, in a packet network, the packets travel from computer to computer until they reach their destination. These computers are called routers. A **router** is a special-purpose computer that interconnects the different computer networks that make up the Internet and routes packets along to their ultimate destination as they travel. To ensure that packets take the best available path toward their destination, routers use a computer program called a **routing algorithm**.

router
special-purpose computer that interconnects the computer networks that make up the Internet and routes packets to their ultimate destination as they travel the Internet

routing algorithm
computer program that ensures that packets take the best available path toward their destination

Packet switching does not require a dedicated circuit, but can make use of any spare capacity that is available on any of several hundred circuits. Packet switching

[2] A bit is a binary digit, 0 or 1. A string of eight bits constitutes a byte. A home telephone dial-up modem connects to the Internet usually at 56 Kbps (56,000 bits per second). Mbps refers to millions of bits per second, whereas Gbps refers to billions of bits per second.

makes nearly full use of almost all available communication lines and capacity. Moreover, if some lines are disabled or too busy, the packets can be sent on any available line that eventually leads to the destination point.

protocol
set of rules and standards for data transfer

Transmission Control Protocol/Internet Protocol (TCP/IP)
core communications protocol for the Internet

TCP
establishes connections among sending and receiving computers and handles assembly and reassembly of packets

IP
provides the Internet's addressing scheme and is responsible for delivery of packets

Network Interface Layer
responsible for placing packets on and receiving them from the network medium

Internet Layer
responsible for addressing, packaging, and routing messages on the Internet

Transport Layer
responsible for providing communication with other protocols within TCP/IP suite

Application Layer
includes protocols used to provide user services or exchange data

Border Gateway Protocol
enables exchange of routing information among systems on the Internet

Transmission Control Protocol/Internet Protocol (TCP/IP)

While packet switching was an enormous advance in communications capacity, there was no universally agreed-upon method for breaking up digital messages into packets, routing them to the proper address, and then reassembling them into a coherent message. This was like having a system for producing stamps but no postal system (a series of post offices and a set of addresses). The answer was to develop a **protocol** (a set of rules and standards for data transfer) to govern the formatting, ordering, compressing, and error-checking of messages, as well as specify the speed of transmission and means by which devices on the network will indicate they have stopped sending and/or receiving messages.

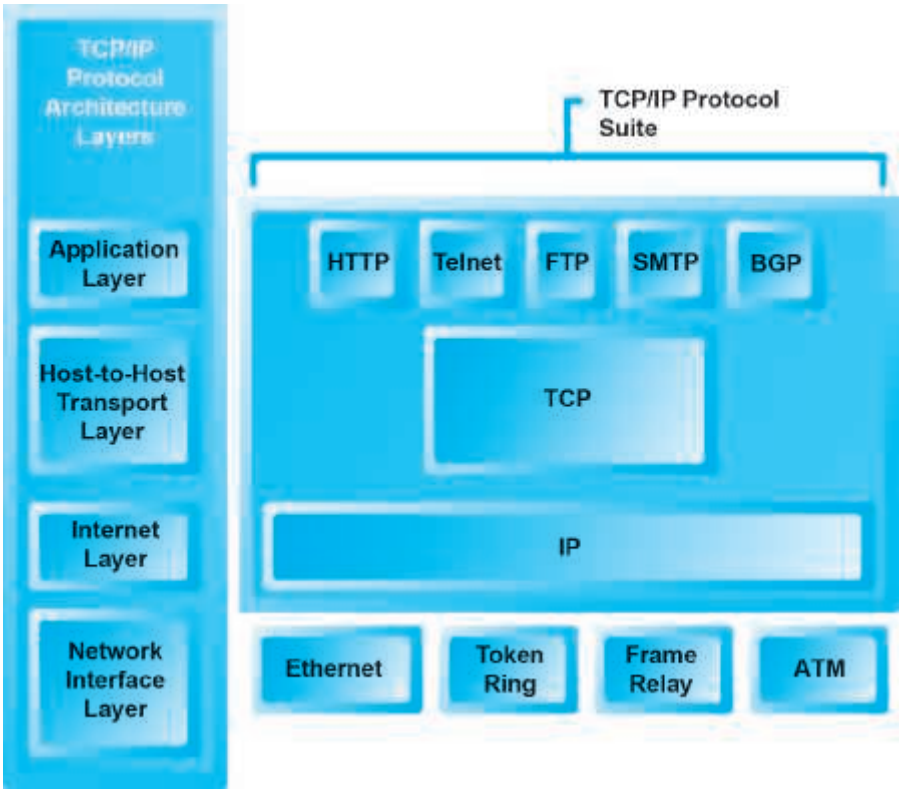
Transmission Control Protocol/Internet Protocol (TCP/IP) has become the core communications protocol for the Internet (Cerf and Kahn, 1974). **TCP** establishes the connections among sending and receiving computers, and makes sure that packets sent by one computer are received in the same sequence by the other, without any packets missing. **IP** provides the Internet's addressing scheme and is responsible for the actual delivery of the packets.

TCP/IP is divided into four separate layers, with each layer handling a different aspect of the communication problem (see **Figure 3.4**). The **Network Interface Layer** is responsible for placing packets on and receiving them from the network medium, which could be a LAN (Ethernet) or Token Ring network, or other network technology. TCP/IP is independent from any local network technology and can adapt to changes at the local level. The **Internet Layer** is responsible for addressing, packaging, and routing messages on the Internet. The **Transport Layer** is responsible for providing communication with other protocols (applications) within the TCP/IP protocol suite by acknowledging and sequencing the packets to and from the applications. The **Application Layer** includes a variety of protocols used to provide user services or exchange data. One of the most important is the **Border Gateway Protocol (BGP)**, which enables the exchange of routing information among different autonomous systems on the Internet. BGP uses TCP as its transport protocol. Other important protocols included in the Application layer include HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP), all of which we will discuss later in this chapter.

IP Addresses

The IP addressing scheme answers the question "How can billions of computers attached to the Internet communicate with one another?" The answer is that every computer connected to the Internet must be assigned an address—otherwise it cannot send or receive TCP packets. For instance, when you sign onto the Internet using a dial-up, DSL, or cable modem, your computer is assigned a temporary address by your

FIGURE 3.4 THE TCP/IP ARCHITECTURE AND PROTOCOL SUITE



TCP/IP is an industry-standard suite of protocols for large internetworks. The purpose of TCP/IP is to provide high-speed communication network links.

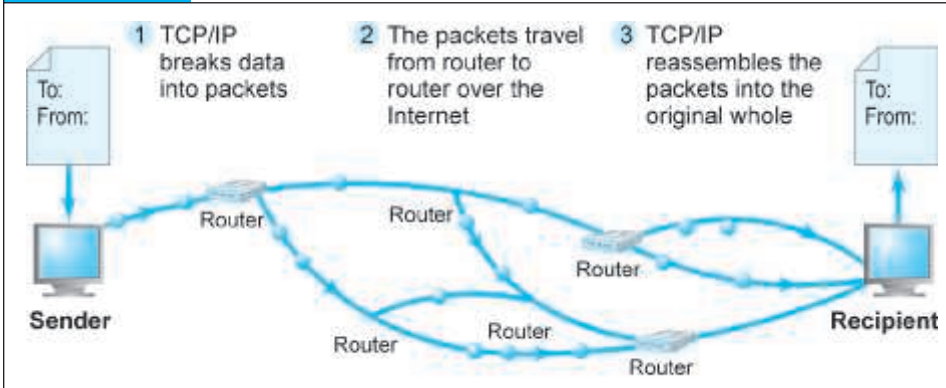
Internet Service Provider. Most corporate and university computers attached to a local area network have a permanent IP address.

There are two versions of IP currently in use: IPv4 and IPv6. An **IPv4 Internet address** is a 32-bit number that appears as a series of four separate numbers marked off by periods, such as 64.49.254.91. Each of the four numbers can range from 0–255. This "dotted quad" addressing scheme supports up to about 4 billion addresses (2 to the 32nd power). In a typical Class C network, the first three sets of numbers identify the network (in the preceding example, 64.49.254 is the local area network identification) and the last number (91) identifies a specific computer.

IPv4 Internet address
Internet address expressed as a 32-bit number that appears as a series of four separate numbers marked off by periods, such as 64.49.254.91

Because many large corporate and government domains have been given millions of IP addresses each (to accommodate their current and future work forces), and with all the new networks and new Internet-enabled devices requiring unique IP addresses being attached to the Internet, the number of IPv4 addresses available to be assigned has shrunk significantly. Registries for North America, Europe, Asia, and Latin

FIGURE 3.5 ROUTING INTERNET MESSAGES: TCP/IP AND PACKET SWITCHING



The Internet uses packet-switched networks and the TCP/IP communications protocol to send, route, and assemble messages. Messages are broken into packets, and packets from the same message can travel along different routes.

IPv6 Internet address
Internet address expressed as a 128-bit number

America have all essentially run out. IPv6 was created to address this problem. An **IPv6 Internet address** is 128 bits, so it can support up to 2^{128} (3.4×10^{38}) addresses, many more than IPv4. According to Akamai, in the United States, about 20% of Internet traffic now occurs over IPv6. Belgium leads the way globally, with over 40% of Internet traffic converted to IPv6 (Akamai, 2016a).

Figure 3.5 illustrates how TCP/IP and packet switching work together to send data over the Internet.

domain name
IP address expressed in natural language

Domain Name System (DNS)
system for expressing numeric IP addresses in natural language

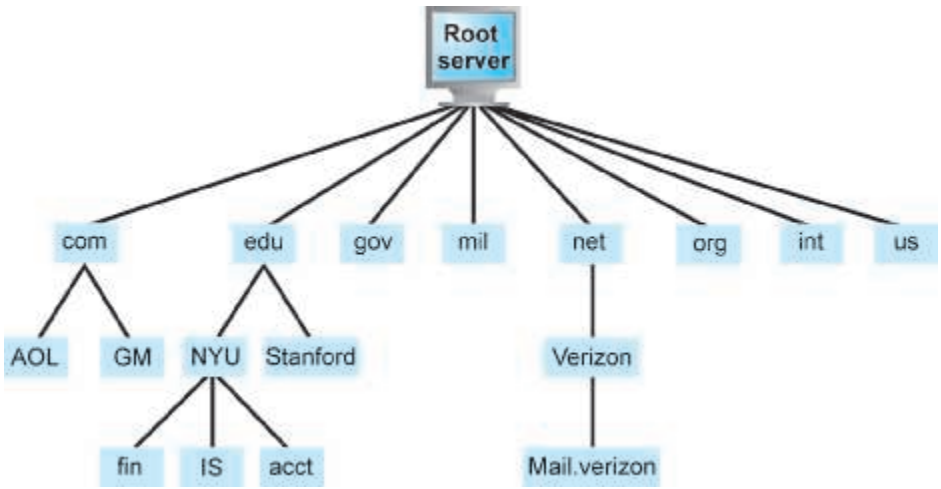
Uniform Resource Locator (URL)
the address used by a web browser to identify the location of content on the Web

Domain Names, DNS, and URLs

Most people cannot remember 32-bit numbers. An IP address can be represented by a natural language convention called a **domain name**. The **Domain Name System (DNS)** allows expressions such as Cnet.com to stand for a numeric IP address (cnet.com's numeric IP is 216.239.113.101).[3] A **Uniform Resource Locator (URL)**, which is the address used by a web browser to identify the location of content on the Web, also uses a domain name as part of the URL. A typical URL contains the protocol to be used when accessing the address, followed by its location. For instance, the URL http://www.azimuth-interactive.com/flash_test refers to the IP address 208.148.84.1 with the domain name "azimuth-interactive.com" and the protocol being used to access the address, HTTP. A resource called "flash_test" is located on the server directory path /flash_test. A URL can have from two to four parts; for example, name1.name2.name3.org. We discuss domain names and URLs further in Section 3.4.

[3] You can check the IP address of any domain name on the Internet. If using a Windows operating system, open the command prompt. Type ping <Domain Name>. You will receive the IP address in return.

FIGURE 3.6 THE HIERARCHICAL DOMAIN NAME SYSTEM



The Domain Name System is a hierarchical namespace with a root server at the top. Top-level domains appear next and identify the organization type (such as .com, .gov, .org, etc.) or geographic location (such as .uk [Great Britain] or .ca [Canada]). Second-level servers for each top-level domain assign and register second-level domain names for organizations and individuals such as IBM.com, Microsoft.com, and Stanford.edu. Finally, third-level domains identify a particular computer or group of computers within an organization, e.g., www.finance.nyu.edu.

Figure 3.6 illustrates the Domain Name System and **Table 3.3** summarizes the important components of the Internet addressing scheme.

Client/Server Computing

While packet switching exploded the available communications capacity and TCP/IP provided the communications rules and regulations, it took a revolution in

TABLE 3.3 PIECES OF THE INTERNET PUZZLE: NAMES AND ADDRESSES

IP addresses	Every device connected to the Internet must have a unique address number called an Internet Protocol (IP) address.
Domain names	The Domain Name System allows expressions such as Pearsoned.com (Pearson Education's website) to stand for numeric IP locations.
DNS servers	DNS servers are databases that keep track of IP addresses and domain names on the Internet.
Root servers	Root servers are central directories that list all domain names currently in use for specific domains; for example, the .com root server. DNS servers consult root servers to look up unfamiliar domain names when routing traffic.

client/server computing
a model of computing in which client computers are connected in a network together with one or more servers

client
a powerful desktop computer that is part of a network

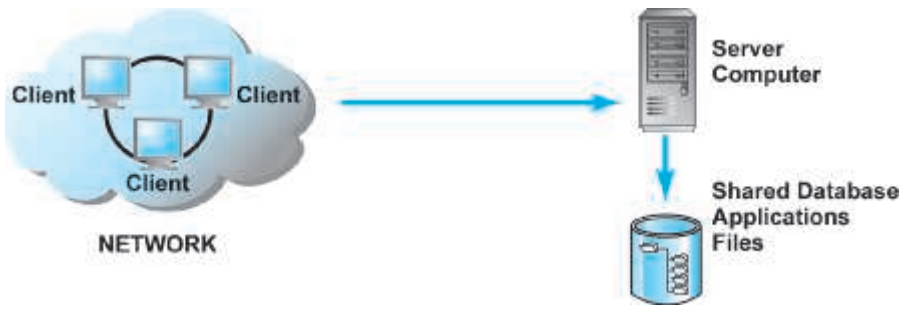
server
networked computer dedicated to common functions that the client computers on the network need

computing to bring about today's Internet and the Web. That revolution is called client/server computing and without it, the Web—in all its richness—would not exist. **Client/server computing** is a model of computing in which **client** computers are connected in a network with one or more **servers**, which are computers that are dedicated to performing common functions that the client computers on the network need, such as file storage, software applications, printing, and Internet access. The client computers are themselves sufficiently powerful to accomplish complex tasks. Servers are networked computers dedicated to common functions that the client computers on the network need, such as file storage, software applications, utility programs that provide web connections, and printers (see **Figure 3.7**). The Internet is a giant example of client/server computing in which millions of web servers located around the world can be easily accessed by millions of client computers, also located throughout the world.

To appreciate what client/server computing makes possible, you must understand what preceded it. In the mainframe computing environment of the 1960s and 1970s, computing power was very expensive and limited. For instance, the largest commercial mainframes of the late 1960s had 128k of RAM and 10-megabyte disk drives, and occupied hundreds of square feet. There was insufficient computing capacity to support graphics or color in text documents, let alone sound files, video, or hyperlinked documents. In this period, computing was entirely centralized: all work was done by a single mainframe computer, and users were connected to the mainframe using terminals.

With the development of personal computers and local area networks during the late 1970s and early 1980s, client/server computing became possible. Client/server computing has many advantages over centralized mainframe computing. For instance, it is easy to expand capacity by adding servers and clients. Also, client/server networks are less vulnerable than centralized computing architectures. If one server goes down,

FIGURE 3.7 THE CLIENT/SERVER COMPUTING MODEL



In the client/server model of computing, client computers are connected in a network together with one or more servers.

backup or mirror servers can pick up the slack; if a client computer is inoperable, the rest of the network continues operating. Moreover, processing load is balanced over many powerful smaller computers rather than being concentrated in a single huge computer that performs processing for everyone. Both software and hardware in client/server environments can be built more simply and economically.

In 2016, there are an estimated 1.8 billion "traditional" personal computers in use around the world (Cox, 2016). Personal computing capabilities have also moved to smartphones and tablet computers (all much "thinner" clients with a bit less computing horsepower, and limited memory, but which rely on Internet servers to accomplish their tasks). In the process, more computer processing will be performed by central servers.

THE NEW CLIENT: THE MOBILE PLATFORM

There's a new client in town. The primary means of accessing the Internet both in the United States and worldwide is now through highly portable smartphones and tablet computers, and not traditional desktop or laptop PCs. This means that the primary platform for e-commerce products and services is also changing to a mobile platform.

The change in hardware has reached a tipping point. The form factor of PCs has changed from desktops to laptops and tablet computers such as the iPad (and more than 100 other competitors). Tablets are lighter, do not require a complex operating system, and rely on the Internet cloud to provide processing and storage. In the United States, about 155 million people access the Internet using a tablet computer (eMarketer, Inc., 2016c).

Smartphones are a disruptive technology that radically alters the personal computing and e-commerce landscape. Smartphones have created a major shift in computer processors and software that has disrupted the dual monopolies long established by Intel and Microsoft, whose chips, operating systems, and software applications began dominating the PC market in 1982. Few smartphones use Intel chips, which power 90% of the world's PCs; only a small percentage of smartphones use Microsoft's operating system (Windows Mobile). Instead, smartphone manufacturers either purchase operating systems such as Symbian, the world leader, or build their own, such as Apple's iPhone iOS, typically based on Linux and Java platforms. Smartphones do not use power-hungry hard drives but instead use flash memory chips with storage up to 128 gigabytes that also require much less power. In 2016, over 210 million Americans use mobile phones to access the Internet (eMarketer, Inc., 2016d).

The mobile platform has profound implications for e-commerce because it influences how, where, and when consumers shop and buy.

THE INTERNET "CLOUD COMPUTING" MODEL: HARDWARE AND SOFTWARE AS A SERVICE

Cloud computing is a model of computing in which computer processing, storage, software, and other services are provided as a shared pool of virtualized resources over the Internet. These "clouds" of computing resources can be accessed on an as-needed

cloud computing
model of computing in which computer processing, storage, software, and other services are provided as a shared pool of virtualized resources over the Internet

FIGURE 3.8 THE CLOUD COMPUTING MODEL

In the cloud computing model, hardware and software services are provided on the Internet by vendors operating very large server farms and data centers.

basis from any connected device and location. **Figure 3.8** illustrates the cloud computing concept.

The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as having the following essential characteristics:

- **On-demand self-service:** Consumers can obtain computing capabilities such as server time or network storage as needed automatically on their own.
- **Ubiquitous network access:** Cloud resources can be accessed using standard network and Internet devices, including mobile platforms.
- **Location-independent resource pooling:** Computing resources are pooled to serve multiple users, with different virtual resources dynamically assigned according to user demand. The user generally does not know where the computing resources are located.
- **Rapid elasticity:** Computing resources can be rapidly provisioned, increased, or decreased to meet changing user demand.
- **Measured service:** Charges for cloud resources are based on the amount of resources actually used.

Cloud computing consists of three basic types of services:

- **Infrastructure as a service (IaaS):** Customers use processing, storage, networking, and other computing resources from third-party providers called cloud service providers (CSPs) to run their information systems. For example, Amazon used the spare capacity of its information technology infrastructure to develop Amazon Web Services (AWS), which offers a cloud environment for a myriad of different IT infrastructure services. See **Table 3.4** for a description of the range of services that AWS offers, such as its Simple Storage Service (S3) for storing customers' data and

TABLE 3.4 AMAZON WEB SERVICES

NAME	DESCRIPTION
COMPUTING SERVICES	
Elastic Compute Cloud (EC2)	Scalable cloud computing services
Elastic Load Balancing (ELB)	Distributes incoming application traffic among multiple EC2 instances
STORAGE SERVICES	
Simple Storage Service (S3)	Data storage infrastructure
Glacier	Low-cost archival and backup storage
DATABASE SERVICES	
DynamoDB	NoSQL database service
Redshift	Petabyte-scale data warehouse service
Relational Database Service (RDS)	Relational database service for MySQL, Oracle, SQL Server, and PostgreSQL databases
ElastiCache	In-memory cache in the cloud
SimpleDB	Non-relational data store
NETWORKING AND CONTENT DELIVERY SERVICES	
Route 53	DNS service in the cloud, enabling business to direct Internet traffic to web applications
Virtual Private Cloud (VPC)	Creates a VPN between the Amazon cloud and a company's existing IT infrastructure
CloudFront	Content delivery services
Direct Connect	Provides alternative to using the Internet to access AWS cloud services
ANALYTICS	
Elastic MapReduce (EMR)	Web service that enables users to perform data-intensive tasks
Kinesis	Big Data service for real-time data streaming ingestion and processing
APPLICATION SERVICES	
AppStream	Provides streaming services for applications and games from the cloud
CloudSearch	Search service that can be integrated by developers into applications
MESSAGING SERVICES	
Simple Email Service (SES)	Cloud e-mail sending service
Simple Notification Service (SNS)	Push messaging service
Simple Queue Service (SQS)	Queue for storing messages as they travel between computers

(continued)

TABLE 3.4 AMAZON WEB SERVICES (CONT.)

DEPLOYMENT AND MANAGEMENT SERVICES	
Identity and Access Management (IAM)	Enables securely controlled access to AWS services
CloudWatch	Monitoring service
Elastic Beanstalk	Service for deploying and scaling web applications and services developed with Java, .Net, PHP, Python, Ruby, and Node.js
CloudFormation	Service that allows developers an easy way to create a collection of related AWS resources
MOBILE	
Cognito	Allows developers to securely manage and synchronize app data for users across mobile devices
Mobile Analytics	Can collect and process billions of events from millions of users a day
PAYMENT SERVICES	
Flexible Payment Service (FPS)	Payment services for developers
DevPay	Online billing and account management service for developers who create an Amazon cloud application
MISCELLANEOUS	
Amazon Mechanical Turk	Marketplace for work that requires human intelligence
Alexa Web Information Service	Provides web traffic data and information for developers

its Elastic Compute Cloud (EC2) service for running applications. Users pay only for the amount of computing and storage capacity they actually use.

- **Software as a service (SaaS):** Customers use software hosted by the vendor on the vendor's cloud infrastructure and delivered as a service over a network. Leading SaaS examples are Google Apps, which provides common business applications online, and Salesforce.com, which provides customer relationship management and related software services over the Internet. Both charge users an annual subscription fee, although Google Apps also has a pared-down free version. Users access these applications from a web browser, and the data and software are maintained on the providers' remote servers.
- **Platform as a service (PaaS):** Customers use infrastructure and programming tools supported by the CSP to develop their own applications. For example, IBM offers Bluemix for software development and testing on its cloud infrastructure. Another example is Salesforce.com's Force.com, which allows developers to build applications that are hosted on its servers as a service.

public cloud
third-party service providers that own and manage large, scalable data centers that offer computing, data storage, and high speed Internet to multiple customers who pay for only the resources they use

A cloud can be private, public, or hybrid. A **public cloud** is owned and maintained by CSPs, such as Amazon Web Services, IBM, HP, and Dell, and made available

to multiple customers, who pay only for the resources they use. A public cloud offers relatively secure enterprise-class reliability at significant cost savings. Because organizations using public clouds do not own the infrastructure, they do not have to make large investments in their own hardware and software. Instead, they purchase their computing services from remote providers and pay only for the amount of computing power they actually use (utility computing) or are billed on a monthly or annual subscription basis. The term *on-demand computing* is also used to describe such services. As such, public clouds are ideal environments for small and medium-sized businesses who cannot afford to fully develop their own infrastructure; for applications requiring high performance, scalability, and availability; for new application development and testing; and for companies that have occasional large computing projects. Gartner estimates that spending on public cloud services worldwide will grow over 15% in 2016, to $204 billion (Gartner, Inc., 2016a). Companies such as Google, Apple, Dropbox, and others also offer public clouds as a consumer service for online storage of data, music, and photos. Google Drive, Dropbox, and Apple iCloud are leading examples of this type of consumer cloud service.

private cloud
provides similar options as public cloud but only to a single tenant

A **private cloud** provides similar options as a public cloud but is operated solely for the benefit of a single tenant. It might be managed by the organization or a third party and hosted either internally or externally. Like public clouds, private clouds can allocate storage, computing power, or other resources seamlessly to provide computing resources on an as-needed basis. Companies that have stringent regulatory compliance or specialized licensing requirements that necessitate high security, such as financial services or healthcare companies, or that want flexible information technology resources and a cloud service model while retaining control over their own IT infrastructure, are gravitating toward these private clouds.

hybrid cloud
offers customers both a public cloud and a private cloud

Large firms are most likely to adopt a **hybrid cloud** computing model, in which they use their own infrastructure for their most essential core activities and adopt public cloud computing for less-critical systems or for additional processing capacity during peak business periods. **Table 3.5** compares the three cloud computing models.

TABLE 3.5 CLOUD COMPUTING MODELS COMPARED

TYPE OF CLOUD	DESCRIPTION	MANAGED BY	USES
Public cloud	Third-party service offering computing, storage, and software services to multiple customers	Third-party service providers (CSPs)	Companies without major privacy concerns Companies seeking pay-as-you-go IT services Companies lacking IT resources and expertise
Private cloud	Cloud infrastructure operated solely for a single organization and hosted either internally or externally	In-house IT or private third-party host	Companies with stringent privacy and security requirements Companies that must have control over data sovereignty
Hybrid cloud	Combination of private and public cloud services that remain separate entities	In-house IT, private host, third-party providers	Companies requiring some in-house control of IT that are also willing to assign part of their IT infrastructures to a public cloud partition on their IT infrastructures

Cloud computing will gradually shift firms from having a fixed infrastructure capacity toward a more flexible infrastructure, some of it owned by the firm, and some of it rented from giant data centers owned by CSPs.

Cloud computing has some drawbacks. Unless users make provisions for storing their data locally, the responsibility for data storage and control is in the hands of the provider. Some companies worry about the security risks related to entrusting their critical data and systems to an outside vendor that also works with other companies. Companies expect their systems to be available 24/7 and do not want to suffer any loss of business capability if cloud infrastructures malfunction. Nevertheless, the trend is for companies to shift more of their computer processing and storage to some form of cloud infrastructure.

Cloud computing has many significant implications for e-commerce. For e-commerce firms, cloud computing radically reduces the cost of building and operating websites because the necessary hardware infrastructure and software can be licensed as a service from CSPs at a fraction of the cost of purchasing these services as products. This means firms can adopt "pay-as-you-go" and "pay-as-you-grow" strategies when building out their websites. For instance, according to Amazon, hundreds of thousands of customers use Amazon Web Services. For individuals, cloud computing means you no longer need a powerful laptop or desktop computer to engage in e-commerce or other activities. Instead, you can use much less-expensive tablet computers or smartphones that cost a few hundred dollars. For corporations, cloud computing means that a significant part of hardware and software costs (infrastructure costs) can be reduced because firms can obtain these services online for a fraction of the cost of owning, and they do not have to hire an IT staff to support the infrastructure.

OTHER INTERNET PROTOCOLS AND UTILITY PROGRAMS

There are many other Internet protocols and utility programs that provide services to users in the form of Internet applications that run on Internet clients and servers. These Internet services are based on universally accepted protocols—or standards—that are available to everyone who uses the Internet. They are not owned by any organization, but they are services that have been developed over many years and made available to all Internet users.

HyperText Transfer Protocol (HTTP)
the Internet protocol used for transferring web pages

HyperText Transfer Protocol (HTTP) is the Internet protocol used to transfer web pages (described in the following section). HTTP was developed by the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF). HTTP runs in the Application Layer of the TCP/IP model shown in Figure 3.4 on page 119. An HTTP session begins when a client's browser requests a resource, such as a web page, from a remote Internet server. When the server responds by sending the page requested, the HTTP session for that object ends. Because web pages may have many objects on them—graphics, sound or video files, frames, and so forth—each object must be requested by a separate HTTP message. For more information about HTTP, you can consult RFC 2616, which details the standards for HTTP/1.1, the version of HTTP most commonly used today (Internet Society, 1999). (An RFC is a document

published by the Internet Society [ISOC] or one of the other organizations involved in Internet governance that sets forth the standards for various Internet-related technologies. You will learn more about the organizations involved in setting standards for the Internet later in the chapter.) An updated version of HTTP, known as HTTP/2, was published as RFC 7540 in May 2015 (IETF, 2015). HTTP/2 addresses a number of HTTP 1.1 shortcomings and is designed to enhance performance by eliminating the need to open multiple TCP connections between a client and server (known as multiplexing), allowing servers to push resources to a client without the client having to request them (known as server push), and reducing the HTTP header size (header compression). HTTP/2 will also have security benefits, with improved performance for encrypted data running over HTTP/2. HTTP/2 is supported by almost all the leading web browsers, but as of August 2016, it has only been adopted by around 10% of the top 10 million websites, in part due to the challenges involved for organizations in transitioning their applications from HTTP to HTTP/2 (Akamai, 2016; W3techs.com, 2016).

E-mail is one of the oldest, most important, and frequently used Internet services. Like HTTP, the various Internet protocols used to handle e-mail all run in the Application Layer of TCP/IP. **Simple Mail Transfer Protocol (SMTP)** is the Internet protocol used to send e-mail to a server. SMTP is a relatively simple, text-based protocol that was developed in the early 1980s. SMTP handles only the sending of e-mail. To retrieve e-mail from a server, the client computer uses either **Post Office Protocol 3 (POP3)** or **Internet Message Access Protocol (IMAP)**. You can set POP3 to retrieve e-mail messages from the server and then delete the messages on the server, or retain them on the server. IMAP is a more current e-mail protocol. IMAP allows users to search, organize, and filter their mail prior to downloading it from the server.

File Transfer Protocol (FTP) is one of the original Internet services. FTP runs in TCP/IP's Application Layer and permits users to transfer files from a server to their client computer, and vice versa. The files can be documents, programs, or large database files. FTP is the fastest and most convenient way to transfer files larger than 1 megabyte, which some e-mail servers will not accept. More information about FTP is available in RFC 959 (Internet Society, 1985).

Telnet is a network protocol that also runs in TCP/IP's Application Layer and is used to allow remote login on another computer. The term Telnet also refers to the Telnet program, which provides the client part of the protocol and enables the client to emulate a mainframe computer terminal. (The industry-standard terminals defined in the days of mainframe computing are VT-52, VT-100, and IBM 3250.) You can then attach yourself to a computer on the Internet that supports Telnet and run programs or download files from that computer. Telnet was the first "remote work" program that permitted users to work on a computer from a remote location.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) are protocols that operate between the Transport and Application Layers of TCP/IP and secure communications between the client and the server. SSL/TLS helps secure e-commerce communications and payments through a variety of techniques, such as message encryption and digital signatures, that we will discuss further in Chapter 5.

Simple Mail Transfer Protocol (SMTP)
the Internet protocol used to send mail to a server

Post Office Protocol 3 (POP3)
a protocol used by the client to retrieve mail from an Internet server

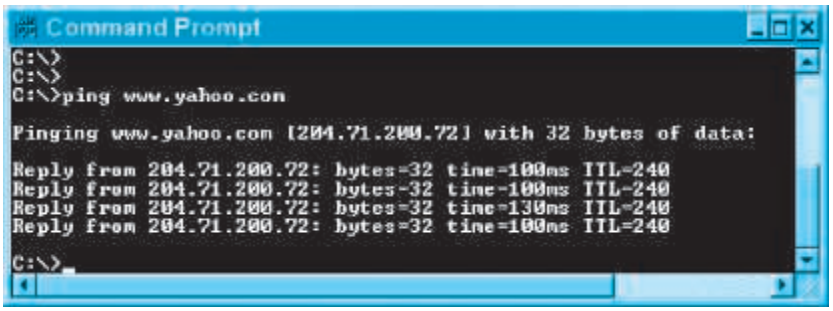
Internet Message Access Protocol (IMAP)
a more current e-mail protocol that allows users to search, organize, and filter their mail prior to downloading it from the server

File Transfer Protocol (FTP)
one of the original Internet services. Part of the TCP/IP protocol that permits users to transfer files from the server to their client computer, and vice versa

Telnet
a terminal emulation program that runs in TCP/IP

Secure Sockets Layer (SSL) /Transport Layer Security (TLS)
protocols that secure communications between the client and the server

FIGURE 3.9 THE RESULT OF A PING



A ping is used to verify an address and test the speed of the round trip from a client computer to a host and back.

SOURCE: Command Prompt, Microsoft Windows, Microsoft Corporation.

Ping
a program that allows you to check the connection between your client and the server

Packet InterNet Groper (Ping) is a utility program that allows you to check the connection between a client computer and a TCP/IP network (see **Figure 3.9**). Ping will also tell you the time it takes for the server to respond, giving you some idea about the speed of the server and the Internet at that moment. You can run Ping from the command prompt on a personal computer with a Windows operating system by typing: ping <domain name>. Ping can also be used to slow down or even crash a domain server by sending it millions of ping requests.

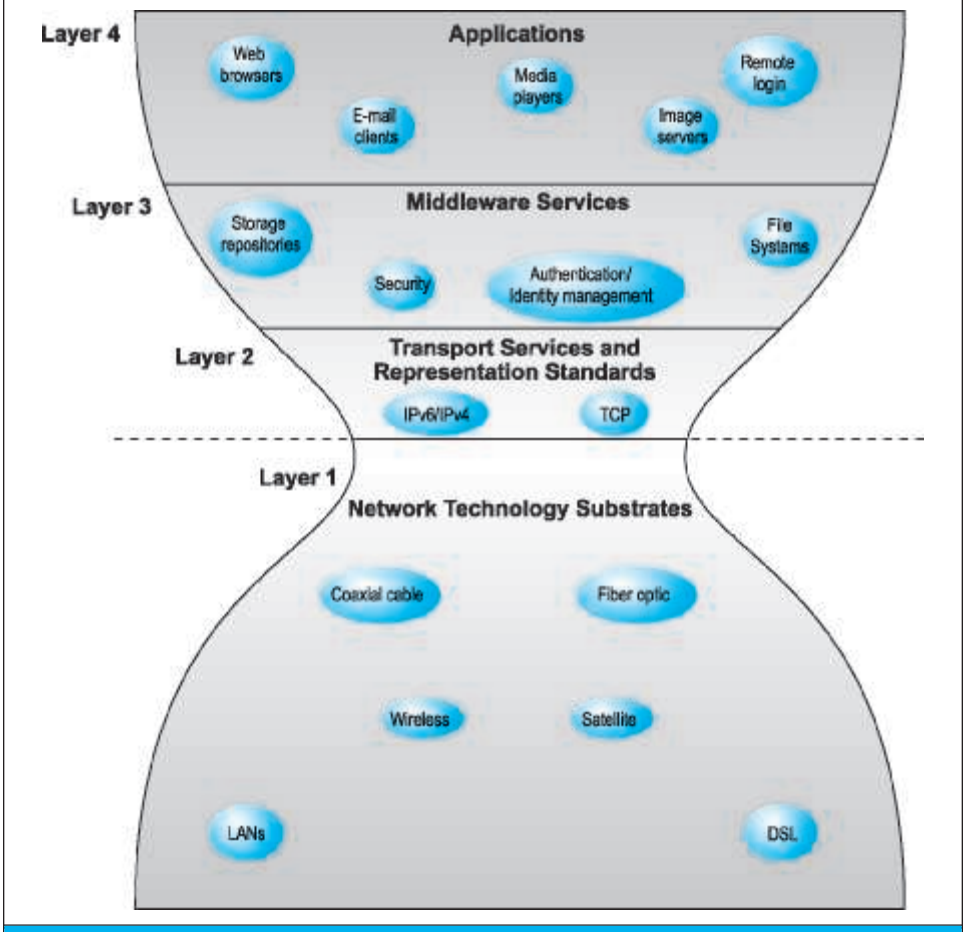
Tracert
one of several route-tracing utilities that allow you to follow the path of a message you send from your client to a remote computer on the Internet

Tracert is one of several route-tracing utilities that allow you to follow the path of a message you send from your client to a remote computer on the Internet. **Figure 3.10** shows the result of a message sent to a remote host using a visual route-tracing program called VisualRoute (available from Visualware).

3.2 THE INTERNET TODAY

In 2016, there are an estimated 3.3 billion Internet users worldwide, up from 100 million users at year-end 1997. While this is a huge number, it still represents less than half (about 45%) of the world's population (eMarketer, Inc., 2016a). Although Internet user growth has slowed in the United States and Western Europe to about 1%–2% annually, worldwide, the growth rate is about 7%, with the highest growth areas being the Middle East/Africa and Asia-Pacific (both still growing at over 8%). By 2020, it is expected that there will be over 3.9 billion Internet users worldwide. One would think the Internet would be overloaded with such incredible growth; however, this has not been true for several reasons. First, client/server computing is highly extensible. By simply adding servers and clients, the population of Internet users can grow indefinitely. Second, the Internet architecture is built in layers so that each layer can change without disturbing developments in other layers. For instance, the technology used to move messages through the Internet can go through radical changes to make service faster without being disruptive to your desktop applications running on the Internet.

FIGURE 3.11 THE HOURGLASS MODEL OF THE INTERNET



The Internet can be characterized as an hourglass modular structure with a lower layer containing the bit-carrying infrastructure (including cables and switches) and an upper layer containing user applications such as e-mail and the Web. In the narrow waist are transportation protocols such as TCP/IP.

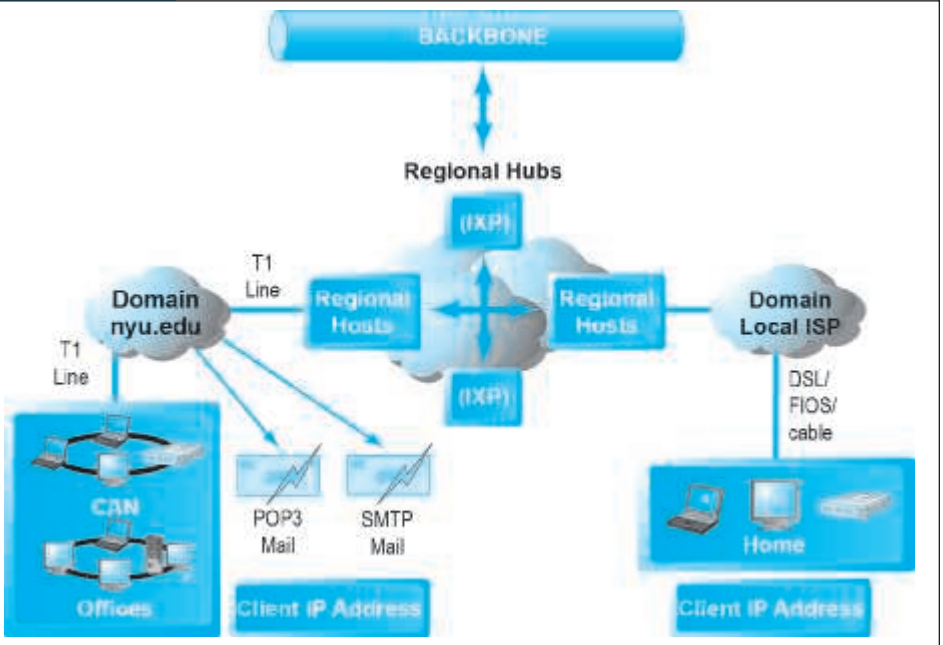
changes in the Network Technology Substrate layer without forcing changes in the Applications layer.

THE INTERNET BACKBONE

Tier 1 Internet Service Providers (Tier 1 ISPs) own and control the major long-haul fiber-optic cable networks comprising the Internet's backbone

Figure 3.12 illustrates some of the main physical elements of today's physical Internet. Originally, the Internet had a single backbone, but today's Internet is woven together from numerous privately owned networks comprised of high-bandwidth fiber-optic cable that are physically connected with each other and that transfer information from one private network to another. These long-haul fiber-optic networks are owned by firms sometimes referred to as **Tier 1 Internet Service Providers (Tier 1 ISPs)** (also sometimes called *transit ISPs*) (see **Table 3.6**). Tier 1 ISPs have "peering"

FIGURE 3.12 INTERNET NETWORK ARCHITECTURE



Today's Internet has a multi-tiered open network architecture featuring multiple backbones, regional hubs, campus/corporate area networks, and local client computers.

arrangements with other Tier 1 ISPs to allow Internet traffic to flow through each other's cables and equipment without charge. Tier 1 ISPs deal only with other Tier 1 or Tier 2 ISPs (described in the next section) and not with end consumers.

For the sake of simplicity, we will refer to these networks of backbones as a single "backbone." The **backbone** has been likened to a giant pipeline that transports data around the world in milliseconds. In the United States, the backbone is composed entirely of fiber-optic cable with bandwidths ranging from 155 Mbps to 2.5 Gbps. **Bandwidth** measures how much data can be transferred over a communications medium within a fixed period of time and is usually expressed in bits per second (Bps), kilobits (thousands of bits) per second (Kbps), megabits (millions of bits) per second (Mbps), or gigabits (billions of bits) per second (Gbps).

backbone
high-bandwidth fiber-optic cable that transports data across the Internet

bandwidth
measures how much data can be transferred over a communications medium within a fixed period of time; is usually expressed in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps)

TABLE 3.6 MAJOR U.S. TIER 1 (TRANSIT) INTERNET SERVICE PROVIDERS

AT&T	Sprint
CenturyLink	Verizon
Cogent Communications	Zayo Group
Level 3 Communications	

Connections to other continents are made via a combination of undersea fiber-optic cable and satellite links. Increasingly, rather than leasing bandwidth from Tier 1 ISPs, Internet giants such as Google, Microsoft, and Facebook are laying down their own fiber-optic networks. For instance, Google has one cable stretching from the California to Japan and another connecting the United States to Brazil, while Facebook and Microsoft have allied to lay a cable across the Atlantic, connecting Virginia to Spain. The backbone in foreign countries typically is operated by a mixture of private and public owners. The backbone has built-in redundancy so that if one part breaks down, data can be rerouted to another part of the backbone. **Redundancy** refers to multiple duplicate devices and paths in a network. A recent study of the Internet's physical structure in the United States has created one of the first maps of the Internet's long-haul fiber network as it currently exists. The map reveals that, not surprisingly, there are dense networks of fiber in the Northeast and coastal areas of the United States, while there is a pronounced absence of infrastructure in the Upper Plains and Four Corners regions. The U.S. Department of Homeland Security has made the map, as well as the data that underlies it, available to government, private, and public researchers, believing that doing so could make the Internet more resilient by improving knowledge (Simonite, 2015; Durairajan et al., 2015).

redundancy
multiple duplicate devices and paths in a network

INTERNET EXCHANGE POINTS

In the United States, there are a number of regional hubs where Tier 1 ISPs physically connect with one another and/or with regional (Tier 2) ISPs. Tier 2 ISPs exchange Internet traffic both through peering arrangements as well as by purchasing Internet transit, and they connect Tier 1 ISPs with Tier 3 ISPs, which provide Internet access to consumers and business. Tier 3 ISPs are described further in the next section. These hubs were originally called Network Access Points (NAPs) or Metropolitan Area Exchanges (MAEs), but now are more commonly referred to as **Internet Exchange Points (IXPs)** (see **Figure 3.13**).

Internet Exchange Point (IXP)
hub where the backbone intersects with local and regional networks and where backbone owners connect with one another

TIER 3 INTERNET SERVICE PROVIDERS

The firms that provide the lowest level of service in the multi-tiered Internet architecture by leasing Internet access to home owners, small businesses, and some large institutions are sometimes called **Tier 3 Internet Service Providers (ISPs)**. Tier 3 ISPs are retail providers. They deal with "the last mile of service" to the curb—homes and business offices. Tier 3 ISPs typically connect to IXPs with high-speed telephone or cable lines (45 Mbps and higher).

Tier 3 Internet Service Provider (Tier 3 ISP)
firm that provides the lowest level of service in the multi-tiered Internet architecture by leasing Internet access to home owners, small businesses, and some large institutions

Three companies, Comcast, Verizon, and Time Warner Cable, together control almost half of the "last mile" wired infrastructure in the United States. Other major Tier 3 ISPs include AT&T, Charter (which is poised to move up the ladder with a proposed purchase, currently awaiting federal approval, of Time Warner Cable and Bright House Networks), Altice (Optimum Online), Cox, Sprint, and CenturyLink. There are also thousands of much smaller, local access ISPs. If you have home or small business Internet access, a Tier 3 ISP likely provides the service to you. (It's important to note that many Tier 3 ISPs are also Tier I ISPs; the two roles are not mutually exclusive.)

FIGURE 3.13 **SOME MAJOR U.S. INTERNET EXCHANGE POINTS (IXPs)**

Region	Name	Location	Operator
EAST	Boston Internet Exchange (BOSIX)	Boston	Markley
	New York International Internet Exchange (NYIIX)	New York	Telehouse
	Peering and Internet Exchange (PAIX)	New York, Virginia, Atlanta	Equinix
	NAP of the Americas	Miami	Verizon Terremark
CENTRAL	Any2 Exchange	Chicago	CoreSite
	Peering and Internet Exchange (PAIX)	Dallas	Equinix
	Midwest Internet Cooperative Exchange (MICE)	Minneapolis	Members
WEST	Peering and Internet Exchange (PAIX)	Seattle, Palo Alto	Equinix
	Los Angeles International Internet Exchange (LAIIX)	Los Angeles	Telehouse
	Any2 Exchange	San Jose, Los Angeles	CoreSite
	Seattle Internet Exchange (SIX)	Seattle	Members

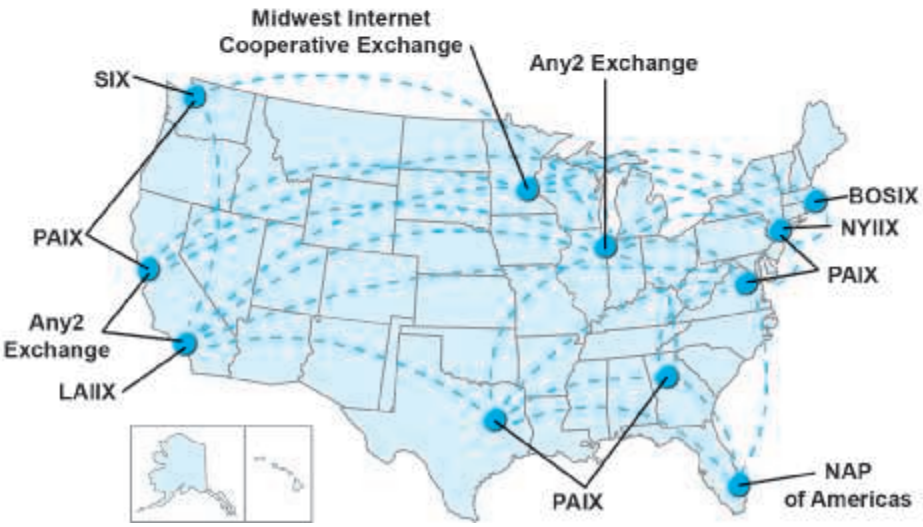


TABLE 3.7 INTERNET ACCESS SERVICE LEVELS AND BANDWIDTH CHOICES

SERVICE	COST/MONTH	DOWNLOAD SPEED
Telephone modem	$10–$25	30–56 Kbps
DSL	$20–$30	1–15 Mbps
FiOS	$50–$300	25 Mbps–500 Mbps
Cable Internet	$35–$199	1 Mbps–500 Mbps
Satellite	$39–$129	5–15 Mbps
T1	$200–$300	1.54 Mbps
T3	$2,500–$10,000	45 Mbps

Satellite firms also offer Internet access, especially in remote areas where broadband service is not available.

Table 3.7 summarizes the variety of services, speeds, and costs of Internet access available to consumers and businesses. There are two types of service: narrowband and broadband. **Narrowband** service is the traditional telephone modem connection now operating at 56.6 Kbps (although the actual throughput hovers around 30 Kbps due to line noise that causes extensive resending of packets). This used to be the most common form of connection worldwide but it has been largely replaced by broadband connections in the United States, Europe, and Asia. Broadband service is based on DSL (including high speed fiber-optic service), cable, telephone (T1 and T3 lines), and satellite technologies. **Broadband**, in the context of Internet service, refers to any communication technology that permits clients to play streaming audio and video files at acceptable speeds. In January 2015, the U.S. Federal Communications Commission updated its broadband benchmark speeds to 25 Mbps for downloads and 3 Mbps for uploads. According to Akamai, the global average connection speed in 2016 was 6.3 Mbps, and the global average peak connection speed was 34.7 Mbps. The United States ranks 16th with an 15.3 Mbps average connection speed (South Korea leads, at 29.9 Mbps) and 22nd with a 67.8 Mbps average peak connection speed (Singapore leads, at 146.9 Mbps) (Akamai, 2016c). The FCC found that 17% of all Americans lack access to 25 Mbps/3 Mbps service, and that rural America is particularly underserved, with more than half lacking such access (Federal Communication Commission, 2015). In the United States, broadband users surpassed dial-up users in 2004, and in 2016, there are an estimated 92 million broadband households (over 75% of all households) (eMarketer, Inc., 2016e).

narrowband
the traditional telephone modem connection, now operating at 56.6 Kbps

broadband
refers to any communication technology that permits clients to play streaming audio and video files at acceptable speeds

The actual throughput of data will depend on a variety of factors including noise in the line and the number of subscribers requesting service. Service-level speeds quoted are typically only for downloads of Internet content; upload speeds tend to be slower, although a number of broadband ISPs have plans that offer the same upload as download speed. T1 and T3 lines are publicly regulated utility lines that offer a

guaranteed level of service, but the actual throughput of the other forms of Internet service is not guaranteed.

Digital Subscriber Line (DSL) service is a telephone technology that provides high-speed access to the Internet through ordinary telephone lines found in a home or business. Service levels typically range from about .5 to 15 Mbps. DSL service requires that customers live within two miles (about 4,000 meters) of a neighborhood telephone switching center. In order to compete with cable companies, telephone companies now also offer an advanced form of DSL called **FiOS (fiber-optic service)** that provides up to 500 Mbps to homes and businesses.

Digital Subscriber Line (DSL)
delivers high-speed access through ordinary telephone lines found in homes or businesses

FiOS (fiber-optic service)
a form of DSL that provides speeds of up to 500 Mbps

Cable Internet refers to a cable television technology that piggybacks digital access to the Internet using the same analog or digital video cable providing television signals to a home. Cable Internet is a major broadband alternative to DSL service, generally providing faster speeds and a "triple play" subscription: telephone, television, and Internet for a single monthly payment. However, the available bandwidth of cable Internet is shared with others in the neighborhood using the same cable. When many people are attempting to access the Internet over the cable at the same time, speeds may slow and performance will suffer. Cable Internet services typically range from 1 Mbps up to 500 Mbps. Comcast, Time Warner Cable, Charter, Cox, and Altice (Optimum Online) are some of the major cable Internet providers.

cable Internet
piggybacks digital access to the Internet on top of the analog video cable providing television signals to a home

T1 and T3 are international telephone standards for digital communication. **T1** lines offer guaranteed delivery at 1.54 Mbps, while **T3** lines offer 45 Mbps. T1 lines cost about $200–$300 per month, and T3 lines around $2500–$6000 per month. These are leased, dedicated, guaranteed lines suitable for corporations, government agencies, and businesses such as ISPs requiring high-speed guaranteed service levels.

T1
an international telephone standard for digital communication that offers guaranteed delivery at 1.54 Mbps

T3
an international telephone standard for digital communication that offers guaranteed delivery at 45 Mbps

Satellite Internet is offered by satellite companies that provide high-speed broadband Internet access primarily to homes and offices located in rural areas where DSL or cable Internet access is not available. Access speeds and monthly costs are comparable to DSL and cable, but typically require a higher initial payment for installation of a small (18-inch) satellite dish. Upload speeds tend to be slower, typically 1–5 Mbps. Satellite providers typically have policies that limit the total megabytes of data that a single account can download within a set period, usually monthly. The major satellite providers are Dish, HughesNet, and Exede. In August 2016, Facebook announced plans to launch a satellite aimed at bringing Internet connectivity to parts of sub-Saharan Africa, but those plans were put on hold when the SpaceX rocket that was to launch the satellite exploded while being tested during pre-launch activities.

satellite Internet
high-speed broadband Internet access provided via satellite

Nearly all business firms and government agencies have broadband connections to the Internet. Demand for broadband service has grown so rapidly because it greatly speeds up the process of downloading web pages and large video and audio files (see **Table 3.8**). As the quality of Internet service offerings continues to expand, the demand for broadband access will continue to swell.

CAMPUS/CORPORATE AREA NETWORKS

Campus/corporate area networks (CANs) are generally local area networks operating within a single organization—such as New York University or Microsoft Corporation. In fact, most large organizations have hundreds of such local area networks.

campus/corporate area network (CAN)
generally, a local area network operating within a single organization that leases access to the Web directly from regional and national carriers

This chapter examines the Internet, Web, and mobile platform of today and tomorrow, how they evolved, how they work, and how their present and future infrastructure enable new business opportunities.

The opening case illustrates the importance of understanding how the Internet and related technologies work, and being aware of what's new. The Internet and its underlying technology are not static phenomena, but instead continue to change over time. Computers have merged with cell phone services; broadband access in the home and broadband wireless access to the Internet via smartphones, tablet computers, and laptops are expanding rapidly; self-publishing via social networks and blogging now engages millions of Internet users; and software technologies such as cloud computing and smartphone apps are revolutionizing the way businesses are using the Internet. Looking forward a few years, the business strategies of the future will require a firm understanding of these technologies and new ones, such as different types of wearable technology like the Apple Watch profiled in the opening case, the Internet of Things, the "smart/connected" movement (smart homes, smart TVs, and connected cars), augmented and virtual reality, and artificial intelligence to deliver products and services to consumers. **Table 3.1** summarizes some of the most important developments in e-commerce infrastructure for 2016–2017.

3.1 THE INTERNET: TECHNOLOGY BACKGROUND

What is the Internet? Where did it come from, and how did it support the growth of the Web? What are the Internet's most important operating principles? How much do you really need to know about the technology of the Internet?

Let's take the last question first. The answer is: it depends on your career interests. If you are on a marketing career path, or general managerial business path, then you need to know the basics about Internet technology, which you'll learn in this and the following chapter. If you are on a technical career path and hope to become a web designer, or pursue a technical career in web infrastructure for businesses, you'll need to start with these basics and then build from there. You'll also need to know about the business side of e-commerce, which you will learn about throughout this book.

Internet
an interconnected network of thousands of networks and millions of computers linking businesses, educational institutions, government agencies, and individuals

As noted in Chapter 1, the **Internet** is an interconnected network of thousands of networks and millions of computers (sometimes called *host computers* or just *hosts*), linking businesses, educational institutions, government agencies, and individuals. The Internet provides approximately 3.3 billion people around the world (including about 267 million people in the United States) with services such as e-mail, apps, newsgroups, shopping, research, instant messaging, music, videos, and news (eMarketer, Inc., 2016a, 2016b). No single organization controls the Internet or how it functions, nor is it owned by anybody, yet it has provided the infrastructure for a transformation in commerce, scientific research, and culture. The word *Internet* is derived from the word *internetwork*, or the connecting together of two or more

TABLE 3.1 TRENDS IN E-COMMERCE INFRASTRUCTURE 2016–2017

BUSINESS
• Mobile devices become the primary access point to social network services and a rapidly expanding social marketing and advertising platform, and create a foundation for location-based web services and business models. • Explosion of Internet content services and mobile access devices strains the business models of Internet backbone providers (the large telecommunication carriers). • The growth in cloud computing and bandwidth capacity enables new business models for distributing music, movies, and television. • Search becomes more social and local, enabling social and local commerce business models. • Big data produced by the Internet creates new business opportunities for firms with the analytic capability to understand it.
TECHNOLOGY
• Mobile devices such as smartphones and tablet computers have become the dominant mode of access to the Internet. The new client is mobile. • The explosion of mobile apps threatens the dominance of the Web as the main source of online software applications and leads some to claim the Web is dead. • Cloud computing reshapes computing and storage, and becomes an important force in the delivery of software applications and online content. • The Internet runs out of IPv4 addresses; the transition to IPv6 continues. • The decreased cost of storage and advances in database software lead to explosion in online data collection known as big data, and creates new business opportunities for firms with the analytic capability to understand it. • The Internet of Things, with millions of sensor-equipped devices connecting to the Internet, starts to become a reality, and is powering the development of smart connected "things" such as televisions, houses, cars, and wearable technology. • Augmented reality applications such as Pokemon GO, and virtual reality hardware such as Facebook's Oculus Rift, Google's Cardboard, and Samsung's Gear VR, begin to gain traction. • Interest in and funding of artificial intelligence technologies explode, with potential applications ranging from supply chain logistics, to self-driving cars, to consumer-oriented personal assistants. • HTML5 grows in popularity among publishers and developers and makes possible web applications that are just as visually rich and lively as native mobile apps.
SOCIETY
• Governance of the Internet becomes more involved with conflicts between nations; the United States gives up control over IANA, which administers the Internet's IP addressing system. • Government control over, and surveillance of, the Internet is expanded in most advanced nations, and in many nations the Internet is nearly completely controlled by government agencies. • The growing infrastructure for tracking online and mobile consumer behavior conflicts with individual claims to privacy and control over personal information.

computer networks. The **Web** is one of the Internet's most popular services, providing access to billions, perhaps trillions, of web pages, which are documents created in a programming language called HTML that can contain text, graphics, audio, video, and other objects, as well as "hyperlinks" that permit users to jump easily from one page to another. Web pages are navigated using web browser software.

Web
one of the Internet's most popular services, providing access to billions, and perhaps trillions, of web pages

THE EVOLUTION OF THE INTERNET: 1961—THE PRESENT

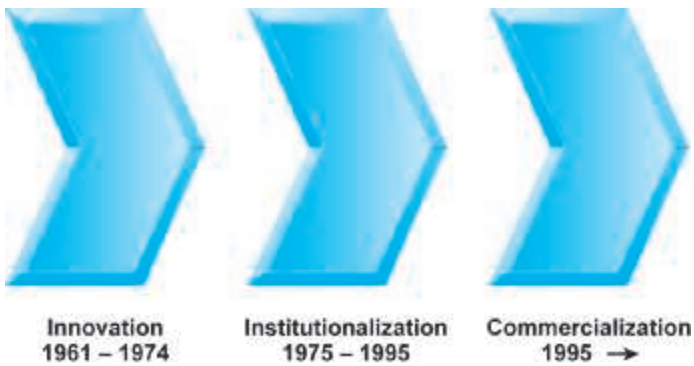
Although journalists talk glibly about "Internet" time—suggesting a fast-paced, nearly instant, worldwide global change mechanism—in fact, today's Internet had its start about 55 years ago and has slowly evolved since then.

The history of the Internet can be segmented into three phases (see **Figure 3.1**). During the *Innovation Phase,* from 1961 to 1974, the fundamental building blocks of the Internet—packet-switching hardware, a communications protocol called TCP/IP, and client/server computing (all described more fully later in this section)—were conceptualized and then implemented in actual hardware and software. The Internet's original purpose was to link large mainframe computers on different college campuses. This kind of one-to-one communication between campuses was previously possible only via the telephone system or private networks owned by the large computer manufacturers.

During the *Institutionalization Phase*, from 1975 to 1995, large institutions such as the U.S. Department of Defense (DoD) and the National Science Foundation (NSF) provided funding and legitimization for the fledging Internet. Once the concepts behind the Internet had been proven in several government-supported demonstration projects, the DoD contributed $1 million to further develop them into a robust military communications system. This effort created what was then called ARPANET (Advanced Research Projects Agency Network). In 1986, the NSF assumed responsibility for the development of a civilian Internet (then called NSFNET) and began a 10-year-long $200 million expansion program.

During the *Commercialization Phase*, from 1995 to the present, the U.S. government encouraged private corporations to take over and expand the Internet backbone as well as local service beyond military installations and college campuses to the rest of the population around the world. See **Table 3.2** for a closer look at the development of the Internet from 1961 on.

FIGURE 3.1 STAGES IN THE DEVELOPMENT OF THE INTERNET



The Internet has developed in three stages over approximately a 55-year period from 1961 to the present. In the Innovation stage, basic ideas and technologies were developed; in the Institutionalization stage, these ideas were brought to life; in the Commercialization stage, once the ideas and technologies had been proven, private companies brought the Internet to millions of people worldwide.

TABLE 3.2 DEVELOPMENT OF THE INTERNET TIMELINE

YEAR	EVENT	SIGNIFICANCE
INNOVATION PHASE 1961–1974		
1961	Leonard Kleinrock (MIT) publishes a paper on "packet switching" networks.	The concept of packet switching is born.
1962	J.C.R. Licklider (MIT) writes memo calling for an "Intergalactic Computer Network."	The vision of a global computer network is born.
1969	BBN Technologies awarded ARPA contract to build ARPANET.	The concept of a packet-switched network moves closer toward physical reality.
1969	The first packet-switched message is sent on ARPANET from UCLA to Stanford.	The communications hardware underlying the Internet is implemented for the first time. The initial ARPANET consisted of four routers (then called Interface Message Processors (IMPs)) at UCLA, Stanford, UCSB, and the University of Utah.
1972	E-mail is invented by Ray Tomlinson of BBN. Larry Roberts writes the first e-mail utility program permitting listing, forwarding, and responding to e-mails.	The first "killer app" of the Internet is born.
1973	Bob Metcalfe (Xerox PARC Labs) invents Ethernet and local area networks.	**Client/server computing is invented.** Ethernet permitted the development of local area networks and client/server computing in which thousands of fully functional desktop computers could be connected into a short-distance (<1,000 meters) network to share files, run applications, and send messages.
1974	"Open architecture" networking and TCP/IP concepts are presented in a paper by Vint Cerf (Stanford) and Bob Kahn (BBN).	**TCP/IP invented.** The conceptual foundation for a single common communications protocol that could potentially connect any of thousands of disparate local area networks and computers, and a common addressing scheme for all computers connected to the network, are born. Prior to this, computers could communicate only if they shared a common proprietary network architecture. With TCP/IP, computers and networks could work together regardless of their local operating systems or network protocols.
INSTITUTIONALIZATION PHASE 1975–1995		
1977	Lawrence Landweber envisions CSNET (Computer Science Network).	CSNET is a pioneering network for U.S. universities and industrial computer research groups that could not directly connect to ARPANET, and was a major milestone on the path to the development of the global Internet.
1980	TCP/IP is officially adopted as the DoD standard communications protocol.	The single largest computing organization in the world adopts TCP/IP and packet-switched network technology.
1980	Personal computers are invented.	Altair, Apple, and IBM personal desktop computers are invented. These computers become the foundation for today's Internet, affording millions of people access to the Internet and the Web.
1984	Apple Computer releases the HyperCard program as part of its graphical user interface operating system called Macintosh.	The concept of "hyperlinked" documents and records that permit the user to jump from one page or record to another is commercially introduced.

(continued)

TABLE 3.2 DEVELOPMENT OF THE INTERNET TIMELINE (CONTINUED)

YEAR	EVENT	SIGNIFICANCE
1984	Domain Name System (DNS) introduced.	DNS provides a user-friendly system for translating IP addresses into words that people can easily understand.
1989	Tim Berners-Lee of CERN in Switzerland proposes a worldwide network of hyperlinked documents based on a common markup language called HTML—HyperText Markup Language.	**The concept of an Internet-supported service called the World Wide Web based on HTML pages is born**. The Web would be constructed from "pages" created in a common markup language, with "hyperlinks" that permitted easy access among the pages.
1990	NSF plans and assumes responsibility for a civilian Internet backbone and creates NSFNET.[1] ARPANET is decommissioned.	The concept of a "civilian" Internet open to all is realized through nonmilitary funding by NSF.
1993	The first graphical web browser called Mosaic is invented by Marc Andreessen and others at the National Center for Supercomputing Applications at the University of Illinois.	Mosaic makes it very easy for ordinary users to connect to HTML documents anywhere on the Web. The browser-enabled Web takes off.
1994	Andreessen and Jim Clark form Netscape Corporation.	The first commercial web browser—Netscape—becomes available.
1994	The first banner advertisements appear on Hotwired.com in October 1994.	**The beginning of e-commerce**.
COMMERCIALIZATION PHASE 1995–PRESENT		
1995	NSF privatizes the backbone, and commercial carriers take over backbone operation.	**The fully commercial civilian Internet is born**. Major long-haul networks such as AT&T, Sprint, GTE, UUNet, and MCI take over operation of the backbone. Network Solutions (a private firm) is given a monopoly to assign Internet addresses.
1995	Jeff Bezos founds Amazon; Pierre Omidyar forms AuctionWeb (eBay).	E-commerce begins in earnest with pure online retail stores and auctions.
1998	The U.S. federal government encourages the founding of the Internet Corporation for Assigned Names and Numbers (ICANN).	Governance over domain names and addresses passes to a private nonprofit international organization.
1999	The first full-service Internet-only bank, First Internet Bank of Indiana, opens for business.	Business on the Web extends into traditional services.
2003	The Internet2 Abilene high-speed network is upgraded to 10 Gbps.	A major milestone toward the development of ultra-high-speed transcontinental networks several times faster than the existing backbone is achieved.
2005	NSF proposes the Global Environment for Network Innovations (GENI) initiative to develop new core functionality for the Internet.	Recognition that future Internet security and functionality needs may require the thorough rethinking of existing Internet technology.
2006	The U.S. Senate Committee on Commerce, Science, and Transportation holds hearings on "Network Neutrality."	The debate grows over differential pricing based on utilization that pits backbone utility owners against online content and service providers and device makers.

[1] "Backbone" refers to the U.S. domestic trunk lines that carry the heavy traffic across the nation, from one metropolitan area to another. Universities are given responsibility for developing their own campus networks that must be connected to the national backbone.

TABLE 3.2 DEVELOPMENT OF THE INTERNET TIMELINE (CONTINUED)

YEAR	EVENT	SIGNIFICANCE
2007	The Apple iPhone is introduced.	The introduction of the iPhone represents the beginning of the development of a viable mobile platform that will ultimately transform the way people interact with the Internet.
2008	The Internet Society (ISOC) identifies Trust and Identity as a primary design element for every layer of the Internet, and launches an initiative to address these issues.	The leading Internet policy group recognizes the current Internet is threatened by breaches of security and trust that are built into the existing network.
2008	Internet "cloud computing" becomes a billion-dollar industry.	Internet capacity is sufficient to support on-demand computing resources (processing and storage), as well as software applications, for large corporations and individuals.
2009	Internet-enabled smartphones become a major new web access platform.	Smartphones extend the reach and range of the Internet to more closely realize the promise of the Internet anywhere, anytime, anyplace.
2009	Broadband stimulus package and Broadband Data Improvement Act enacted.	President Obama signs stimulus package containing $7.2 billion for the expansion of broadband access in the United States.
2011	ICANN expands domain name system.	ICANN agrees to permit the expansion of generic top-level domain names from about 300 to potentially thousands using any word in any language.
2012	World IPv6 Launch day.	Major Internet service providers (ISPs), home networking equipment manufacturers, and online companies begin to permanently enable IPv6 for their products and services as of June 6, 2012.
2013	The Internet of Things (IoT) starts to become a reality.	Internet technology spreads beyond the computer and mobile device to anything that can be equipped with sensors, leading to predictions that up to 100–200 billion uniquely identifiable objects will be connected to the Internet by 2020.
2014	Apple introduces Apple Pay and Apple Watch.	Apple Pay is likely to become the first widely adopted mobile payment system; Apple Watch may usher in a new era of wearable Internet-connected technology and is a further harbinger of the Internet of Things.
2015	Federal Communications Commission adopts regulations mandating net neutrality.	ISPs are required to treat all data on the Internet equally and are not allowed to discriminate or charge differentially based on user, content, site, platform, application, type of equipment, or mode of communication.
2016	FCC proposes "Open Set Top Box" rules; net neutrality regulations upheld by U.S. Court of Appeals.	FCC continues to promote concept of an open Internet, despite continued resistance from telecommunications industry.

SOURCES: Based on Leiner et al., 2000; Zakon, 2005; Gross, 2005; Geni.net, 2007; ISOC.org, 2010; Arstechnica.com, 2010; ICANN, 2011a; Internet Society, 2012; IEEE Computer Society, 2013; Craig, 2016.

web client
any computing device attached to the Internet that is capable of making HTTP requests and displaying HTML pages, most commonly a Windows PC or Macintosh

A **web client**, on the other hand, is any computing device attached to the Internet that is capable of making HTTP requests and displaying HTML pages. The most common client is a Windows or Macintosh desktop computer, with various flavors of Unix/Linux computers a distant third. However, the fastest growing category of web clients is not computers at all, but mobile devices. In general, a web client can be any device—including a printer, refrigerator, stove, home lighting system, or automobile instrument panel—capable of sending and receiving information from a web server.

WEB BROWSERS

web browser
software program whose primary purpose is to display web pages

A **web browser** is a software program whose primary purpose is to display web pages. Browsers also have added features, such as e-mail and newsgroups (an online discussion group or forum). As of July 2016, the leading desktop web browser is Google's Chrome, a small, yet technologically advanced open source browser, with about 51% of the market. Chrome is also the leading mobile/tablet browser, with about a 52% share of that market. The second most popular desktop browser is Microsoft's Internet Explorer, with about a 30% share. However, Internet Explorer's share of the mobile/tablet market is miniscule, with less than a 2% share. Mozilla Firefox is in third place in the desktop browser marketplace, with only about 8% share. It has less than a 1% share of the mobile/tablet browser market. First released in 2004, Firefox is a free, open source web browser for the Windows, Linux, and Macintosh operating systems, based on Mozilla open source code (which originally provided the code for Netscape). It is small and fast and offers many features such as pop-up blocking and tabbed browsing. Apple's Safari browser has only about a 4.5% share of the desktop browser market, but is the second most popular mobile/tablet browser, with a 28% share, due in large part to its use on iPhones and iPads (Marketshare.hitslink.com, 2016a, 2016b). In 2015, Microsoft introduced Edge, an entirely new browser bundled with its new operating system, Windows 10. Edge was designed to replace Internet Explorer. However, despite the popularity of Windows 10, Edge has thus far been largely ignored by Windows 10 adopters and has been installed on only about 5% of desktops.

3.5 THE INTERNET AND THE WEB: FEATURES AND SERVICES

The Internet and the Web have spawned a number of powerful software applications upon which the foundations of e-commerce are built. You can think of all these as web services, and it is interesting as you read along to compare these services to other traditional media such as television or print media. If you do, you will quickly realize the richness of the Internet environment.

COMMUNICATION TOOLS

The Internet and Web provide a number of communication tools that enable people around the globe to communicate with one another, both on a one-to-one basis as well

as a one-to-many basis. Communication tools include e-mail, messaging applications, online message boards (forums), Internet telephony applications, and video conferencing, video chatting, and telepresence. We'll look at each of these in a bit more depth in the following sections.

E-mail

Since its earliest days, **electronic mail**, or **e-mail**, has been the most-used application of the Internet. Worldwide, there are over 2.6 billion e-mail users, sending over 2.15 billion e-mails a day. There are an estimated 1.7 billion mobile e-mail users worldwide, with over 65% of all e-mail users worldwide accessing e-mail on a mobile device (Radicati Group, 2016). Estimates vary on the amount of spam, ranging from 40% to 90%. E-mail marketing and spam are examined in more depth in Chapter 6.

electronic mail (e-mail)
the most-used application of the Internet. Uses a series of protocols to enable messages containing text, images, sound, and video clips to be transferred from one Internet user to another

E-mail uses a series of protocols to enable messages containing text, images, sound, and video clips to be transferred from one Internet user to another. Because of its flexibility and speed, it is now the most popular form of business communication—more popular than the phone, fax, or snail mail (the U.S. Postal Service). In addition to text typed within the message, e-mail also allows **attachments**, which are files inserted within the e-mail message. The files can be documents, images, sounds, or video clips.

attachment
a file inserted within an e-mail message

Messaging Applications

Instant messaging (IM) allows you to send messages in real time,unlike e-mail, which has a time lag of several seconds to minutes between when messages are sent and received. IM displays text entered almost instantaneously. Recipients can then respond immediately to the sender the same way, making the communication more like a live conversation than is possible through e-mail. To use IM, users create a buddy list they want to communicate with, and then enter short text messages that their buddies will receive instantly (if they are online at the time). And although text remains the primary communication mechanism in IM, more advanced systems also provide voice and video chat functionality. Instant messaging over the Internet competes with cell phone Short Message Service (SMS) and Multimedia Messaging Service (MMS) texting, which is far more expensive than IM. Major IM systems include Skype, Yahoo Messenger, Google Hangouts, and AIM (AOL Instant Messenger). IM systems were initially developed as proprietary systems, with competing firms offering versions that did not work with one another. Today, there still is no built-in interoperability among the major IM systems.

instant messaging (IM)
displays text entered almost instantaneously. Recipients can then respond immediately to the sender the same way, making the communication more like a live conversation than is possible through e-mail

Mobile messaging apps, such as Facebook Messenger, WhatsApp (purchased by Facebook for $22 billion in 2014), Snapchat (which allows users to send pictures, videos, and texts that will disappear after a short period of time), Kik, Viber, and others have also become wildly popular, providing competition for both traditional desktop IM systems and SMS text messaging. In the United States in 2016, over 130 million people (about 40% of the population) use mobile messaging apps, and companies are increasingly turning their attention to using these apps to market their brands (eMarketer, Inc., 2016g).

Online Message Boards

online message board a web application that allows Internet users to communicate with each other, although not in real time

An **online message board** (also referred to as a forum, bulletin board, discussion board, discussion group, or simply a board or forum) is a web application that enables Internet users to communicate with each other, although not in real time. A message board provides a container for various discussions (or "threads") started (or "posted") by members of the board, and depending on the permissions granted to board members by the board's administrator, enables a person to start a thread and reply to other people's threads. Most message board software allows more than one message board to be created. The board administrator typically can edit, delete, move, or otherwise modify any thread on the board. Unlike an electronic mailing list (such as a listserv), which automatically sends new messages to a subscriber, an online message board typically requires that the member visit the board to check for new posts. Some boards offer an "e-mail notification" feature that notifies users that a new post of interest to them has been made.

Internet Telephony

If the telephone system were to be built from scratch today, it would be an Internet-based, packet-switched network using TCP/IP because it would be less expensive and more efficient than the alternative existing system, which involves a mix of circuit-switched legs with a digital backbone. In fact, AT&T has begun testing all-digital IP phone networks in several U.S. cities. Likewise, if cable television systems were built from scratch today, they most likely would use Internet technologies for the same reasons.

IP telephony a general term for the technologies that use VoIP and the Internet's packet-switched network to transmit voice and other forms of audio communication over the Internet

Voice over Internet Protocol (VoIP) protocol that allows for transmission of voice and other forms of audio communication over the Internet

IP telephony is a general term for the technologies that use **Voice over Internet Protocol (VoIP)** and the Internet's packet-switched network to transmit voice, fax, and other forms of audio communication over the Internet. VoIP can be used over a traditional handset as well as over a mobile device. VoIP avoids the long distance charges imposed by traditional phone companies.

There were about 230 million residential VoIP subscribers worldwide in 2015, and in the United States, more than half of residential customers are now using VoIP, and this number is expanding rapidly as cable systems provide telephone service as part of their "triple play": voice, Internet, and TV as a single package. This number is dwarfed, however, by the number of mobile VoIP subscribers, which has grown explosively over the last several years, fueled by the rampant growth of mobile messaging apps that now also provide free VoIP services, such as Facebook Messenger, WhatsApp (also owned by Facebook), Viber (owned by Japanese e-commerce giant Rakuten), WeChat, Line, KakaoTalk, and others (IHS, 2016; BuddeComm, 2016).

VoIP is a disruptive technology. In the past, voice and fax were the exclusive provenance of the regulated telephone networks. With the convergence of the Internet and telephony, however, this dominance is already starting to change, with local and long distance telephone providers and cable companies becoming ISPs, and ISPs getting into the phone market. Key players in the VoiP market include independent service providers such as VoIP pioneers Vonage and Skype (now owned by Microsoft), as well as traditional players such as telephone and cable companies that have moved aggressively into the market. Skype currently dominates the international market.

Skype carries over 3 billion minutes per day (translating into about 90 billion minutes per month) from 300 million users around the world (Anurag, 2016).

Video Conferencing, Video Chatting, and Telepresence

Internet video conferencing is accessible to anyone with a broadband Internet connection and a web camera (webcam). The most widely used web conferencing suite of tools is WebEx (now owned by Cisco). VoIP companies such as Skype and ooVoo also provide more limited web conferencing capabilities, commonly referred to as video chatting. Apple's FaceTime is another video chatting technology available for iOS mobile devices with a forward-facing camera and Macintosh computers equipped with Apple's version of a webcam, called a FaceTime camera.

Telepresence takes video conferencing up several notches. Rather than single persons "meeting" by using webcams, telepresence creates an environment in a room using multiple cameras and screens, which surround the users. The experience is uncanny and strange at first because as you look at the people in the screens, they are looking directly at you. Broadcast quality and higher screen resolutions help create the effect. Users have the sensation of "being in the presence of their colleagues" in a way that is not true for traditional webcam meetings. Providers of telepresence software and hardware include Cisco, LifeSize, BlueJeans Network, and Polycom ATX.

SEARCH ENGINES

Search engines identify web pages that appear to match keywords, also called queries, entered by a user and then provide a list of the best matches (search results). Almost 85% of U.S. Internet users regularly use search engines from either desktop or mobile devices, and they generate around 16 billion queries a month on desktop computers, about 10.2 billion of which are conducted using Google. Desktop search volume is declining, as more and more search activity moves to mobile devices. In fact, Google has reported that mobile search queries exceeded desktop queries in the United States and numerous other countries for the first time in 2015 (eMarketer, Inc., 2016h, 2016i; Sterling, 2016). There are hundreds of different search engines, but the vast majority of the search results are supplied by the top three providers: Google, Microsoft's Bing, and Yahoo. Google currently has about 64% of the desktop search market based on number of searches, followed by Microsoft's Bing, with about 22%, and Yahoo with about 12%.

search engine
identifies web pages that appear to match keywords, also called queries, entered by the user and then provides a list of the best matches

Web search engines started out in the early 1990s shortly after Netscape released the first commercial web browser. Early search engines were relatively simple software programs that roamed the nascent Web, visiting pages and gathering information about the content of each web page. These early programs were called variously crawlers, spiders, and wanderers; the first full-text crawler that indexed the contents of an entire web page was called WebCrawler, released in 1994. AltaVista (1995), one of the first widely used search engines, was the first to allow "natural language" queries such as "history of web search engines" rather than "history + web + search engine."

The first search engines employed simple keyword indexes of all the web pages visited. They would count the number of times a word appeared on the web page, and store this information in an index. These search engines could be easily fooled by web

designers who simply repeated words on their home pages. The real innovations in search engine development occurred through a program funded by the Department of Defense called the Digital Library Initiative, designed to help the Pentagon find research papers in large databases. Stanford, Berkeley, and three other universities became hotbeds of web search innovations in the mid-1990s. At Stanford in 1994, two computer science students, David Filo and Jerry Yang, created a hand-selected list of their favorite web pages and called it "Yet Another Hierarchical Officious Oracle," or Yahoo!. Yahoo initially was not a real search engine, but rather an edited selection of web sites organized by categories the editors found useful. Yahoo later developed "true" search engine capabilities.

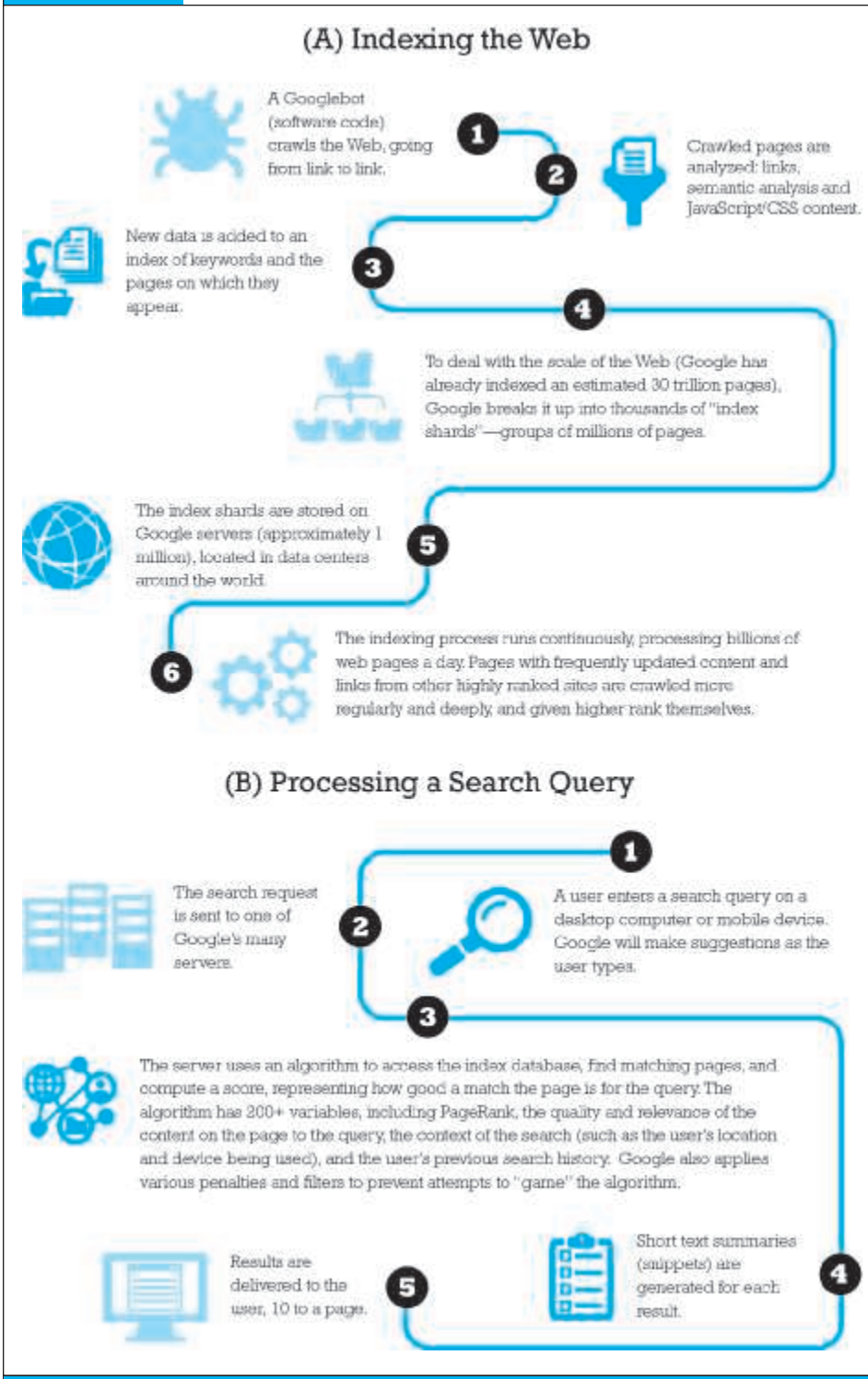
In 1998, Larry Page and Sergey Brin, two Stanford computer science students, released their first version of the Google search engine. This search engine was different: not only did it index each web page's words, but Page had discovered that the AltaVista search engine not only collected keywords from sites but also calculated what other sites linked to each page. By looking at the URLs on each web page, they could calculate an index of popularity. AltaVista did nothing with this information. Page took this idea and made it a central factor in ranking a web page's appropriateness to a search query. He patented the idea of a web page ranking system (PageRank System), which essentially measures the popularity of the web page. Brin contributed a unique web crawler program that indexed not just keywords on a web page, but combinations of words (such as authors and their article titles). These two ideas became the foundation for the Google search engine (Brandt, 2004). **Figure 3.18(A)** illustrates how Google indexes the Web. **Figure 3.18(B)** shows you what happens when you enter a search query.

Initially, few understood how to make money from search engines. That changed in 2000 when Goto.com (later Overture) allowed advertisers to bid for placement on their search engine results, and Google followed suit in 2003 with its AdWords program, which allowed advertisers to bid for placement of short text ads on Google search results. The spectacular increase in Internet advertising revenues (which have been growing at around 20%–25% annually over the last few years) has helped search engines transform themselves into major shopping tools and created an entire new industry called "search engine marketing."

When users enter a search term at Google, Bing, Yahoo, or any of the other websites serviced by these search engines, they receive two types of listings: sponsored links, for which advertisers have paid to be listed (usually at the top of the search results page), and unsponsored "organic" search results. Advertisers can also purchase small text ads on the right side of the search results page. In addition, search engines have extended their services to include news, maps, satellite images, computer images, e-mail, group calendars, group meeting tools, and indexes of scholarly papers.

Although the major search engines are used for locating general information of interest to users, search engines have also become a crucial tool within e-commerce sites. Customers can more easily search for the product information they want with the help of an internal search program; the difference is that within websites, the search engine is limited to finding matches from that one site. For instance, more online shoppers use Amazon's internal search engine to look for products than conducting a

FIGURE 3.18 HOW GOOGLE WORKS



product search using Google, a fact noted by Google's executive chairman Eric Schmidt, who believes that Amazon search poses a significant threat to Google (Mangalindan, 2014). Pinterest hopes to challenge Google in the realm of visual search, as discussed in the closing case study in Chapter 1.

DOWNLOADABLE AND STREAMING MEDIA

download
transfers a file from a web server and stores it on a computer for later use

streaming media
enables video, music, and other large-bandwidth files to be sent to a user in a variety of ways that enable the user to play the files as they are being delivered

When you **download** a file from the Web, the file is transferred from a web server and is stored on your computer for later use. With the low-bandwidth connections of the early Internet, audio and video files were difficult to download, but with the huge growth in broadband connections, these files are not only commonplace but today constitute the majority of web traffic. **Streaming media** is an alternative to downloaded media and enables video, music, and other large-bandwidth files to be sent to a user in a variety of ways that enable the user to play the files as they are being delivered. In some situations, the files are broken into chunks and served by specialized video servers to client software that puts the chunks together and plays the video. In other situations, a single large file is delivered from a standard web server to a user who can begin playing the video before the entire file is delivered. Streamed files must be viewed in real time; they cannot be stored on client hard drives without special software. Streamed files are "played" by a software program such as Windows Media Player, Apple QuickTime, Adobe Flash, and Real Player. There are a number of tools used to create streaming files, including HTML5 and Adobe Flash, as well as technologies specifically adapted for the mobile platform such as the Meerkat and Periscope apps. As the capacity of the Internet grows, streaming media will play an even larger role in e-commerce.

Spurred on by the worldwide sales of more than 2.5 billion iOS (iPhones, iPads, and iPod Touches) and Android devices, the Internet has become a virtual digital river of music, audio, and video files. The Apple iTunes store is probably the most well-known repository of digital music online, with a catalog of more than 43 million songs worldwide in its catalog as of September 2016. Google Play offers over 35 million, and there are hundreds of other sites offering music downloads as well. In addition, streaming music services and Internet radio, such as Apple Music, Spotify, Pandora, Amazon Prime Music, Tidal, and hundreds of others, add to the bandwidth devoted to the delivery of online music.

podcast
an audio presentation—such as a radio show, audio from a movie, or simply a personal audio presentation—stored online as a digital media file

Podcasting (the name originates from a mashup of the word "iPod" and the word "broadcasting") is also surging in popularity. A **podcast** is an audio presentation—such as a radio show, audio from a conference, or simply a personal presentation—stored online as digital media file. Listeners can download the file and play it on their mobile devices or computers. Podcasting has transitioned from an amateur independent producer media in the "pirate radio" tradition to a professional news and talk content distribution channel. For instance, This American Life's *Serial* podcast has been downloaded over 175 million times. NPR is the top U.S. producer of podcasts, with an aggregate monthly audience of almost 8 million, followed by WNYC Studios, a NYC-based public broadcasting organization, with a monthly audience of about 6 million (Podtrac, Inc., 2016).

Online video viewing has also exploded in popularity. In 2016, for instance, there are around 215 million Americans that watch streaming or downloaded video content on a desktop or mobile device at least once a month (eMarketer, Inc., 2016j). Cisco estimates that consumer Internet video traffic constituted a whopping 70% of all consumer Internet traffic in 2015, and this percentage is expected to grow to 82% by 2020 (Cisco, 2016b). The Internet has become a major distribution channel for movies, television shows, and sporting events (see Chapter 10). Another common type of Internet video is provided by YouTube, with more than 1 billion users worldwide, who each day watch hundreds of millions of hours of video content, ranging from a wide variety of user-generated content, to branded content from major corporations, music videos, original programming, and more. Sites such as YouTube, Metacafe, and Facebook have popularized user-generated video streaming. Many apps such as Instagram, Twitter, Snapchat, and others also include video capabilities.

Online advertisers increasingly use video to attract viewers. Companies that want to demonstrate use of their products have found video clips to be extremely effective. Streaming video segments used in web ads and news stories are perhaps the most frequently used streaming services. High-quality interactive video and audio makes sales presentations and demonstrations more effective and lifelike and enables companies to develop new forms of customer support.

WEB 2.0 APPLICATIONS AND SERVICES

Today's broadband Internet infrastructure has greatly expanded the services available to users. These capabilities have formed the basis for new business models. Web 2.0 applications and services are "social" in nature because they support communication among individuals within groups or social networks.

Online Social Networks

Online social networks are services that support communication within networks of friends, colleagues, and entire professions. Online social networks have developed very large worldwide audiences (over 2.3 billion people in 2016, almost one-third of the world's population) and form the basis for new advertising platforms and for social e-commerce (see Chapters 6, 7, and 11). The largest social networks are Facebook (1.7 billion monthly active users worldwide), Instagram (500 million members worldwide), LinkedIn (more than 450 million members worldwide), Twitter (more than 310 million active users worldwide), and Pinterest (over 110 million active users). These networks rely on user-generated content (messages, photos, and videos) and emphasize sharing of content. All of these features require significant broadband Internet connectivity and equally large cloud computing facilities to store content.

Blogs

blog
personal web page that is created by an individual or corporation to communicate with readers

A **blog** (originally called a **weblog**) is a personal web page that typically contains a series of chronological entries (newest to oldest) by its author, and links to related web pages. The blog may include a blogroll (a collection of links to other blogs) and

trackbacks (a list of entries in other blogs that refer to a post on the first blog). Most blogs allow readers to post comments on the blog entries as well. The act of creating a blog is often referred to as "blogging." Blogs are either hosted by a third-party site such as WordPress, Tumblr, Blogger, LiveJournal, TypePad, and Xanga, or prospective bloggers can download software such as Movable Type to create a blog that is hosted by the user's ISP. Blog pages are usually variations on templates provided by the blogging service or software and hence require no knowledge of HTML. Therefore, millions of people without HTML skills of any kind can post their own web pages, and share content with friends and relatives. The totality of blog-related websites is often referred to as the "blogosphere."

Blogs have become hugely popular. Tumblr and Wordpress together hosted over 400 million blogs as of September 2016, so it is likely that the total number is significantly higher. According to eMarketer, there are an estimated 29 million active U.S. bloggers, and 81 million U.S. blog readers (eMarketer, Inc., 2916k, 2016l). No one knows how many of these blogs are kept up to date or are just yesterday's news. And no one knows how many of these blogs have a readership greater than one (the blog author). In fact, there are so many blogs you need a search engine just to find them, or you can just go to a list of the most popular 100 blogs and dig in.

Wikis

wiki
web application that allows a user to easily add and edit content on a web page

A **wiki** is a web application that allows a user to easily add and edit content on a web page. (The term wiki derives from the "wiki wiki" (quick or fast) shuttle buses at Honolulu Airport.) Wiki software enables documents to be written collectively and collaboratively. Most wiki systems are open source, server-side systems that store content in a relational database. The software typically provides a template that defines layout and elements common to all pages, displays user-editable source code (usually plain text), and then renders the content into an HTML-based page for display in a web browser. Some wiki software allows only basic text formatting, whereas others allow the use of tables, images, or even interactive elements, such as polls and games. Because wikis by their very nature are very open in allowing anyone to make changes to a page, most wikis provide a means to verify the validity of changes via a "Recent Changes" page, which enables members of the wiki community to monitor and review the work of other users, correct mistakes, and hopefully deter "vandalism."

The most well-known wiki is Wikipedia, an online encyclopedia that contains more than 40 million articles in 294 different languages on a variety of topics. The Wikimedia Foundation, which operates Wikipedia, also operates a variety of related projects, including Wikibooks, a collection of collaboratively written free textbooks and manuals; Wikinews, a free content news source; and Wiktionary, a collaborative project to produce a free multilingual dictionary in every language, with definitions, etymologies, pronunciations, quotations, and synonyms.

VIRTUAL REALITY AND AUGMENTED REALITY

virtual reality (VR)
involves fully immersing users within a virtual world, typically through the use of a head-mounted display (HMD) connected to headphones and other devices

In 2016, virtual reality and augmented reality technologies began to enter the consumer market and attract significant attention. **Virtual reality (VR)** involves fully immersing users within a virtual world, typically through the use of a head-mounted

display (HMD) connected to headphones and other devices that enable navigation through the experience and allowing users to feel as if they are actually present within the virtual world. High-end VR devices designed to be used with PCs or gaming systems include Facebook's Oculus Rift, HTC's Vive, and Sony's PlayStation VR. Samsung's Gear VR and Google Cardboard are examples of lower-cost, mobile, entry-level devices. A number of publishers are experimented with VR content that can use these lower-cost devices. For example, the New York Times has a VR mobile app that viewers can use with Google Cardboard to view VR films and advertisements that feature 360-degree video. By 2020, some analysts estimate that there will be almost 155 million virtual reality users worldwide (with around 135 million using a smartphone-powered device and another 20 million a higher-end PC/game console-related device). **Augmented reality (AR)** involves overlaying virtual objects over the real world, via smartphones, tablets, or HMDs. Perhaps the highest profile use of AR thus far has been its use in Nintendo's Pokemon GO game. Other uses include Snapchat's Lenses feature, which uses facial recognition technology and 3-D models that allow users to augment their selfies by overlaying animations or other images on top of them, and "try-before-you-buy" apps created for beauty and fashion brands (eMarketer, Inc., 2016m).

augmented reality (AR)
involves overlaying virtual objects over the real world, via smartphones, tablets or HMDs.

INTELLIGENT PERSONAL ASSISTANTS

The idea of having a conversation with a computer, having it understand you and be able to carry out tasks according to your direction, has long been a part of science fiction, from the 1968 Hollywood movie *2001: A Space Odyssey*, to an old Apple promotional video depicting a professor using his personal digital assistant to organize his life, gather data, and place orders at restaurants. That was all fantasy. But Apple's Siri, billed as an intelligent personal assistant and knowledge navigator and released in 2011, has many of the capabilities of the computer assistants found in fiction. Siri has a natural language, conversational interface, situational awareness, and is capable of carrying out many tasks based on verbal commands by delegating requests to a variety of different web services. For instance, you can ask Siri to find a restaurant nearby that serves Italian food. Siri may show you an ad for a local restaurant in the process. Once you have identified a restaurant you would like to eat at, you can ask Siri to make a reservation using OpenTable. You can also ask Siri to place an appointment on your calendar, search for airline flights, and figure out what's the fastest route between your current location and a destination using public transit. The answers are not always completely accurate, but critics have been impressed with its uncanny abilities. Siri is currently available on the Apple Watch, the iPhone 4S and later versions, iPads with Retina display, the iPad Mini, and iPod Touches (fifth generation and later versions).

In 2012, Google released its version of an intelligent assistant for Android-based smartphones, which it calls Google Now. Google Now is part of the Google Search mobile application. While Google Now has many of the capabilities of Apple's Siri, it attempts to go further by predicting what users may need based on situational awareness, including physical location, time of day, previous location history, calendar, and expressed interests based on previous activity, as described in its patent application (United States Patent Office, 2012). For instance, if you often search for a particular musician or style of music, Google Now might provide recommendations for similar

music. If it knows that you go to a health club every other day, Google Now will remind you not to schedule events during these periods. If it knows that you typically read articles about health issues, the system might monitor Google News for similar articles and make recommendations. In 2016, Google unveiled Google Assistant, a similar virtual assistant for its Allo chat app and integrated into its Google Home products and its new Pixel phones. Other intelligent personal assistants include Samsung's S Voice, LG's Voice Mate, and Microsoft's Cortana. The *Insight on Business* case, *AI, Intelligent Assistants, and Chatbots*, focuses on the increasing use of AI technologies in e-commerce.

3.6 MOBILE APPS: THE NEXT BIG THING IS HERE

When Steve Jobs introduced the iPhone in January 2007, no one, including himself, envisioned that the device would launch a software revolution or become a major e-commerce platform, let alone a game platform, advertising platform, and general media platform for television shows, movies, videos, and e-books. The iPhone's original primary functions, beyond being a cell phone, were to be a camera, text messaging device, and web browser. What Apple initially lacked for the iPhone were software applications ("apps") that would take full advantage of its computing capabilities. The solution was apps developed by outside developers. In July 2008, Apple introduced the App Store, which provides a platform for the distribution and sale of apps by Apple as well as by independent developers. Around the same time, Google was developing Android as an open source operating system for mobile devices. In October 2008, the first smartphone using Android was released, and Google launched the Android Market (now called Google Play) as the official app store for Android. In 2010, tablet computers such as Apple's iPad and the Samsung Galaxy Tab, which provided additional platforms for mobile apps, were introduced.

As of June 2016, more than 130 billion apps have been downloaded from the App Store, and there are over 2 million approved apps available for download. There are over 2 million apps available for Android devices on Google Play as well. And while the number of cumulative downloads of Android apps is not publicly available, Google has announced that Android users downloaded over 65 billion apps between May 2015 and May 2016 alone.

The mobile app phenomenon has spawned a new digital ecosystem: tens of thousands of developers, a wildly popular hardware platform, and millions of consumers now using a mobile device to replace their clunky desktop-laptop Microsoft Windows computer and act as a digital media center as well. Mobile apps have even usurped TV as the most popular entertainment medium. A 2015 report from Flurry found that the average U.S. consumer now spends nearly 200 minutes per day within apps, well ahead of the 168 minutes spent watching TV. As recently as 2014, TV was still comfortably ahead of apps. More consumers are opting to consume media on their phones and tablet computers than ever before, which is more good news for app developers.

INSIGHT ON BUSINESS

AI, INTELLIGENT ASSISTANTS, AND CHATBOTS

Despite the frequent appearances of robots and advanced artificial intelligence (AI) in books and movies over the past several decades, real-world equivalents have lagged hopelessly behind. However, today's tech titans are doubling their efforts to improve AI technologies in an effort to get a jump on the competition. We may still be a long way away from R2-D2, but AI in the form of personalization systems, chatbots, and intelligent assistants is finally entering the mainstream.

AI systems of the past have had frustratingly limited capabilities. Asking them to perform tasks outside of their purpose or to interpret and respond to the variation and nuances of human language simply doesn't work. Even tools like search engines, which have the ability to distinguish between different types of language and queries, can't incorporate context.

Although companies like Amazon have made use of more complex forms of AI to power their personalization and recommendation engines, this mostly occurs behind the scenes—customers aren't interacting directly with these types of AI technologies. However, advances in natural language processing techniques have enabled Amazon to develop exciting new technologies like the Amazon Echo and its underlying AI technology, which Amazon calls Alexa. The Echo is marketed as a home assistant that can perform a variety of tasks using speech recognition, but is still in its infancy as a product. Currently, the Echo can update to-do lists, adjust home appliances, play games, and stream music, all controlled by voice.

Echo and Alexa are powered by these and other "skills," which function much like apps do on the iPhone, and which third-party developers are lining up in droves to develop. For example, 1-800-Flowers was one of the first large retailers to develop a skill that allows users to place orders by voice alone on any device running Alexa, including the Echo and the Amazon Fire TV. Although customers interested in using this capability must have account info, payment info, and addresses already on file, this represents a major breakthrough. Other companies developing skills for Alexa include Domino's, Capital One, Ford Motor, and many more. Amazon is hoping that in the future, people will be able to ask Alexa what they should buy and receive an intelligent, relevant response.

Although Echo and Alexa are perhaps the most visible sign of growth in artificial intelligence and natural language processing, the modern technological landscape is defined by its multitude of platforms. Retailers are trying to encourage their customers to do business with them on each and every one of them. Many of these platforms are text-based, and the number of people using messaging apps is skyrocketing in the United States, from 113 million in 2015 to a projected 177 million by 2019. To that end, companies have been rolling out "chatbots"—AI that can interact with users via text and automate many parts of the purchasing process that are currently manual, such as talking on the phone or navigating online menus.

Facebook Messenger is one of the most popular messaging apps, trailing only WhatsApp in monthly active users. Facebook M is a virtual assistant within Messenger launched in 2015 that can perform a variety of tasks via text, including making restaurant reservations, booking travel plans, and helping find birthday gifts. Facebook has also opened the Messenger platform to third-party chatbots from other companies, including the previously mentioned 1-800-Flowers as well

(continued)

as others like Uber. Increasingly, popular workplace messaging tool Slack has done the same with its platform, and companies like Taco Bell have developed tools like TacoBot that allow Slack users to order food through a brief text conversation.

Seemingly every prominent tech company and messaging platform has an AI that it hopes will dominate the emerging marketplace. Amazon has Alexa and Facebook has M; Apple has Siri, perhaps the best known intelligent assistant; Google has Google Now and Google Assistant; Microsoft has Cortana. Google also unveiled its Google Home appliance, which is modeled after the Echo but which reportedly has better conversational functionality and ability to integrate with home speakers. In the same vein, Samsung announced the Samsung Otto device, which comes equipped with features Echo lacks like an HD camera and facial recognition capability. These companies are all positioning themselves to take part in the impending boom in virtual assistant technologies. Analysts anticipate that virtual assistants of all types will have 1.8 billion active global users by 2021, up from 390 million in 2016.

Other players have emerged as well. The developers of the AI that powers Apple's Siri have developed a new platform called Viv that goes far beyond Siri's functionality. Viv can answer much more complicated questions than Siri, such as "Will it be warmer than 70 degrees near the Golden Gate Bridge after 5 PM the day after tomorrow?" Viv can also book flights by using your preferred airline, frequent flyer number, and seating preference, all without any human guidance, and might someday have the ability to automatically detect low fares.

A primary goal of all of these technologies is to facilitate sales. Intelligent personal assistants and chatbots might be able to understand what it is that we're looking for as consumers even when we're not sure how to phrase it or what we're even looking for. If AI continues to improve and people learn to trust technologies like chatbots, the importance of websites and native apps is likely to greatly diminish, and web search may also take a hit. That's part of the reason why Google has been so active in this area, perhaps sensing a threat to its core business model.

Interestingly, Microsoft has eight full-time writers who formulate Cortana's responses to user queries. The team's goal is for Cortana to exhibit the type of multi-dimensional intelligence that humans display—social intelligence, emotion, humor, and a point of view. Whichever intelligent assistant is most successful at this is likely to have a leg up on the others. Although these technologies still require plenty of human guidance (Facebook M reportedly has a staff of human customer service agents on hand to handle difficult queries), the time may finally have arrived where interacting directly with AI becomes a part of our everyday lives.

SOURCES: "What Alexa & AI Means for the Future of Commerce," by Richard MacManus, Richardmacmanus.com, August 25, 2016; "Why Dominos' Virtual Assistant Struggles to Understand Your Orders," by Clint Boulton, Cio.com, August 24, 2016; "What Retailers Need to Know, and Expect, About Virtual Digital Technology," by Judy Motti, Retailcustomerexperience.com, August 5, 2016; "3 Ways Artificial Intelligence Is Transforming E-commerce," by Ben Rossi, Information-age.com, July 18, 2016; "These Three Virtual Assistants Point the Way to the Future," by Mike Elgan, Computerworld.com, June 8, 2016; "The Search for the Killer Bot," by Sharon Gaudin, Casey Newton, Theverge.com, June 1, 2016; "When a Robot Books Your Airline Ticket," by Jane L. Levere, *New York Times,* May 30, 2016; "Google Makes Push Into Artificial Intelligence with New Offerings," by Jack Nicas, *Wall Street Journal,* May 18, 2016; "Google Home vs. Amazon Echo: Why Home Could Win," by Andrew Gebhart, Cnet.com, May 18, 2016; "New Siri Sibling Viv May Be Next Step in A.I. Evolution," Computerworld.com, May 11, 2016; "Siri-Creator Shows Off First Public Demo of Viv, 'The Intelligent Interface for Everything,'" by Lucas Matney, Techcrunch.com, May 9, 2016; "1-800-Flowers Chats Up Amazon's Alexa," by Allison Enright, Internetretailer.com, April 26, 2016; "The Chatbots are Coming - and They Want to Help You Buy Stuff," by Sarah Halzack, *Washington Post*, April 13, 2016; "What Can Chatbots Do for Ecommerce?" by Mike O'Brien, Clickz.com, April 11, 2016; "2 Ways Artificial Intelligence Is Changing Customer Engagement," by Randy Kohl, The-future-of-commerce.com, February 18, 2016; "How Real People Help Cortana, Siri, and Other Virtual Assistants Feel Alive," by Mike Elgan, Pcworld.com, February 1, 2016; "The North Face Brings AI to Ecommerce," by Rebecca Harris, Marketingmag.ca, January 12, 2016.

The implications of the app ecosystem for e-commerce are significant. The smartphone in your pocket or the tablet computer on your lap becomes not only a general-purpose computer, but also an always-present shopping tool for consumers, as well as an entirely new marketing and advertising platform for vendors. Early e-commerce applications using desktops and laptops were celebrated as allowing people to shop in their pajamas. Smartphones and tablets extend this range from pajamas to office desktops to trains, planes, and cars, all fully clothed. You can shop anywhere, shop everywhere, and shop all the time, in between talking, texting, watching video, and listening to music. Almost all of the top 100 brands have a presence in at least one of the major app stores, and more than 90% have an app in the Apple App Store. M-commerce in the form of purchases of retail and travel products and services via a mobile device is expected to generate over $180 billion in 2016, while downloads of mobile apps and in-app purchases are expected to generate over $10 billion (eMarketer, Inc., 2016n, 2016o, 2016p).

PLATFORMS FOR MOBILE APPLICATION DEVELOPMENT

Unlike mobile web sites, which can be accessed by any web-enabled mobile device, native apps, which are designed specifically to operate using the mobile device's hardware and operating system, are platform-specific. Applications for the iPhone, iPad, and other iOS devices are written in the Objective-C programming language using the iOS SDK (software developer kit). Applications for Android operating system–based phones typically are written using Java, although portions of the code may be in the C or C++ programming language. Applications for Windows mobile devices are written in C or C++. In addition to creating native apps using a programming language such as Objective C or Java, there are also hundreds of low-cost or open source app development toolkits that make creating cross-platform mobile apps relatively easy and inexpensive without having to use a device-specific programming language. See Section 4.6 in Chapter 4 for more information.

APP MARKETPLACES

Once written, applications are distributed through various marketplaces. Android apps for Android-based phones are distributed through Google Play, which is controlled by Google. iPhone applications are distributed through Apple's App Store. Microsoft operates the Windows Phone Marketplace for Windows mobile devices. Apps can also be purchased from third-party vendors such as Amazon's Appstore. It is important to distinguish "native" mobile apps, which run directly on a mobile device and rely on the device's internal operating system, from web apps, which install into your browser, although these can operate in a mobile environment as well.

As *Cyberwar: MAD 2.0* illustrates, the Internet and Web are increasingly vulnerable to large-scale attacks and potentially large-scale failure. Increasingly, these attacks are led by organized gangs of criminals operating globally—an unintended consequence of globalization. Even more worrisome is the growing number of large-scale attacks that are funded, organized, and led by various nations against the Internet resources of other nations. Anticipating and countering these attacks has proved a difficult task for both business and government organizations. However, there are several steps you can take to protect your websites, your mobile devices, and your personal information from routine security attacks. Reading this chapter, you should also start thinking about how your business could survive in the event of a large-scale "outage" of the Internet.

In this chapter, we will examine e-commerce security and payment issues. First, we will identify the major security risks and their costs, and describe the variety of solutions currently available. Then, we will look at the major payment methods and consider how to achieve a secure payment environment. **Table 5.1** highlights some of the major trends in online security in 2016–2017.

TABLE 5.1 WHAT'S NEW IN E-COMMERCE SECURITY 2016–2017

- Large-scale data breaches continue to expose data about individuals to hackers and other cybercriminals.
- Mobile malware presents a tangible threat as smartphones and other mobile devices become more common targets of cybercriminals, especially as their use for mobile payments rises.
- Malware creation continues to skyrocket and ransomware attacks rise.
- Distributed Denial of Service (DDoS) attacks are now capable of slowing Internet service within entire countries.
- Nations continue to engage in cyberwarfare and cyberespionage.
- Hackers and cybercriminals continue to focus their efforts on social network sites to exploit potential victims through social engineering and hacking attacks.
- Politically motivated, targeted attacks by hacktivist groups continue, in some cases merging with financially motivated cybercriminals to target financial systems with advanced persistent threats.
- Software vulnerabilities, such as the Heartbleed bug and other zero day vulnerabilities, continue to create security threats.
- Incidents involving celebrities raise awareness of cloud security issues.

5.1 THE E-COMMERCE SECURITY ENVIRONMENT

For most law-abiding citizens, the Internet holds the promise of a huge and convenient global marketplace, providing access to people, goods, services, and businesses worldwide, all at a bargain price. For criminals, the Internet has created entirely new—and lucrative—ways to steal from the more than 1.6 billion Internet consumers

worldwide in 2016. From products and services, to cash, to information, it's all there for the taking on the Internet.

It's also less risky to steal online. Rather than rob a bank in person, the Internet makes it possible to rob people remotely and almost anonymously. Rather than steal a CD at a local record store, you can download the same music for free and almost without risk from the Internet. The potential for anonymity on the Internet cloaks many criminals in legitimate-looking identities, allowing them to place fraudulent orders with online merchants, steal information by intercepting e-mail, or simply shut down e-commerce sites by using software viruses and swarm attacks. The Internet was never designed to be a global marketplace with billions of users and lacks many basic security features found in older networks such as the telephone system or broadcast television networks. By comparison, the Internet is an open, vulnerable-design network. The actions of cybercriminals are costly for both businesses and consumers, who are then subjected to higher prices and additional security measures. The costs of malicious cyberactivity include not just the cost of the actual crime, but also the additional costs that are required to secure networks and recover from cyberattacks, the potential reputational damage to the affected company, as well as reduced trust in online activities, the loss of potentially sensitive business information, including intellectual property and confidential business information, and the cost of opportunities lost due to service disruptions. Ponemon Institute estimates that the average total cost of a data breach to U.S. corporations in 2016 was $4 million (Ponemon Institute, 2016).

THE SCOPE OF THE PROBLEM

Cybercrime is becoming a more significant problem for both organizations and consumers. Bot networks, DDoS attacks, Trojans, phishing, ransomware, data theft, identity fraud, credit card fraud, and spyware are just some of the threats that are making daily headlines. Social networks also have had security breaches. But despite the increasing attention being paid to cybercrime, it is difficult to accurately estimate the actual amount of such crime, in part because many companies are hesitant to report it due to the fear of losing the trust of their customers, and because even if crime is reported, it may be difficult to quantify the actual dollar amount of the loss. A 2014 study by the Center for Strategic and International Studies examined the difficulties in accurately estimating the economic impact of cybercrime and cyberespionage, with its research indicating a range of $375 billion to $575 billion worldwide. Further research is planned to try to help determine an even more accurate estimate (Center for Strategic and International Studies, 2014).

One source of information is a survey conducted by Ponemon Institute of 58 representative U.S. companies in various industries. The 2015 survey found that the average annualized cost of cybercrime for the organizations in the study was $15 million, representing a 20% increase from the previous year, and an 82% increase since the first survey in 2009. The average cost per attack was more than $1.9 million, a 22% increase from the previous year. The number of successful cyberattacks also increased, by over 15%. The most costly cybercrimes were those caused by denial of service, malicious insiders, and malicious code. The most prevalent types of attacks were viruses, worms, and Trojans, experienced by 100% of the companies surveyed, followed by malware

(97%), web-based attacks (76%), botnets (66%), phishing and social engineering attacks (59%), and malicious code (52%) (Ponemon Institute, 2015a).

Reports issued by security product providers, such as Symantec, are another source of data. Symantec issues a semi-annual *Internet Security Threat Report*, based on 57.6 million sensors monitoring Internet activity in more than 157 countries. Advances in technology have greatly reduced the entry costs and skills required to enter the cybercrime business. Low-cost and readily available web attack kits enable hackers to create malware without having to write software from scratch. In addition, there has been a surge in polymorphic malware, which enables attackers to generate a unique version of the malware for each victim, making it much more difficult for pattern-matching software used by security firms to detect. According to Symantec, the number of data breaches increased 23% in 2015, over half a billion personal records were stolen, the number of spear-phishing attacks increased by 55%, malware increased by 36%, and ransomware attacks grew by 35% (Symantec, 2016). However, Symantec does not attempt to quantify actual crimes and/or losses related to these threats.

Online credit card fraud is one of the most high-profile forms of e-commerce crime. Although the average amount of credit card fraud loss experienced by any one individual is typically relatively small, the overall amount is substantial. The overall rate of online credit card fraud is estimated to be about 0.8% of all online card transactions, including both mobile and web transactions (Cybersource, 2016). The nature of credit card fraud has changed greatly from the theft of a single credit card number and efforts to purchase goods at a few sites, to the simultaneous theft of millions of credit card numbers and their distributions to thousands of criminals operating as gangs of thieves. The emergence of identity fraud, described in detail later in this chapter, as a major online/offline type of fraud may well increase markedly the incidence and amount of credit card fraud, because identity fraud often includes the use of stolen credit card information and the creation of phony credit card accounts.

The Underground Economy Marketplace: The Value of Stolen Information

Criminals who steal information on the Internet do not always use this information themselves, but instead derive value by selling the information to others on the so-called underground or shadow economy market. Data is currency to cybercriminals and has a "street value" that can be monetized. For example, in 2013, Vladislav Horohorin (alias "BadB") was sentenced to over 7 years in federal prison for using online criminal forums to sell stolen credit and debit card information (referred to as "dumps"). At the time of his arrest, Horohorin possessed over 2.5 million stolen credit and debit card numbers. There are several thousand known underground economy marketplaces around the world that sell stolen information, as well as malware, such as exploit kits, access to botnets, and more. **Table 5.2** lists some recently observed prices for various types of stolen data, which typically vary depending on the quantity being purchased, supply available, and "freshness." For example, when credit card information from the Target data breach first appeared on the market, individual card numbers went for up to $120 each. After a few weeks, however, the price dropped

TABLE 5.2 THE CYBER BLACK MARKET FOR STOLEN DATA

DATA	PRICE*
Individual U.S. card number with expiration date and CVV2 (the three-digit number printed on back of card) (referred to as a CVV)	$5–$8
Individual U.S. card number with full information, including full name, billing address, expiration date, CVV2, date of birth, mother's maiden name, etc. (referred to as a Fullz or Fullzinfo)	$30
Dump data for U.S. card (the term "dump" refers to raw data such as name, account number, expiration data, and CVV encoded on the magnetic strip on the back of the card)	$110–$120
Online payment service accounts	$20–$300
Bank account login credentials	$80–$700
Online account login credentials (Facebook, Twitter, eBay)	$10–$15
Medical information/health credentials	$10–$20
1,000 e-mail addresses	$1–$10
Scan of a passport	$1–$2

SOURCES: Based on data from McAfee, 2016; Intel Security, 2015; Symantec, 2015; Maruca, 2015; Infosec Institute, 2015; RAND Corporation, 2014.

*Prices vary based on supply and quality (freshness of data, account balances, validity, etc.).

dramatically (Leger, 2014). Experts believe the cost of stolen information has generally fallen as the tools of harvesting have increased the supply. On the demand side, the same efficiencies and opportunities provided by new technology have increased the number of people who want to use stolen information. It's a robust marketplace.

Finding these marketplaces and the servers that host them can be difficult for the average user (and for law enforcement agencies), and prospective participants are typically vetted by other criminals before access is granted. This vetting process takes place through Twitter, Tor, and VPN services, and sometimes e-mail exchanges of information, money (often Bitcoins, a form of digital cash that we discuss further in Section 5.5 and in the *Insight on Business* case study on pages 315–316), and reputation. There is a general hierarchy of cybercriminals in the marketplace, with low-level, nontechnical criminals who frequent "carder forums," where stolen credit and debit card data is sold, aiming to make money, a political statement, or both, at the bottom; resellers in the middle acting as intermediaries; and the technical masterminds who create malicious code at the top.

So, what can we can conclude about the overall size of cybercrime? Cybercrime against e-commerce sites is dynamic and changing all the time, with new risks appearing often. The amount of losses to businesses is significant and growing. The managers of e-commerce sites must prepare for an ever-changing variety of criminal assaults, and keep current in the latest security techniques.

WHAT IS GOOD E-COMMERCE SECURITY?

What is a secure commercial transaction? Anytime you go into a marketplace you take risks, including the loss of privacy (information about what you purchased). Your prime risk as a consumer is that you do not get what you paid for. As a merchant in the market, your risk is that you don't get paid for what you sell. Thieves take merchandise and then either walk off without paying anything, or pay you with a fraudulent instrument, stolen credit card, or forged currency.

E-commerce merchants and consumers face many of the same risks as participants in traditional commerce, albeit in a new digital environment. Theft is theft, regardless of whether it is digital theft or traditional theft. Burglary, breaking and entering, embezzlement, trespass, malicious destruction, vandalism—all crimes in a traditional commercial environment—are also present in e-commerce. However, reducing risks in e-commerce is a complex process that involves new technologies, organizational policies and procedures, and new laws and industry standards that empower law enforcement officials to investigate and prosecute offenders. **Figure 5.1** illustrates the multi-layered nature of e-commerce security.

To achieve the highest degree of security possible, new technologies are available and should be used. But these technologies by themselves do not solve the problem. Organizational policies and procedures are required to ensure the technologies are not subverted. Finally, industry standards and government laws are required to enforce payment mechanisms, as well as to investigate and prosecute violators of laws designed to protect the transfer of property in commercial transactions.

FIGURE 5.1 THE E-COMMERCE SECURITY ENVIRONMENT

E-commerce security is multi-layered, and must take into account new technology, policies and procedures, and laws and industry standards.

The history of security in commercial transactions teaches that any security system can be broken if enough resources are put against it. Security is not absolute. In addition, perfect security of every item is not needed forever, especially in the information age. There is a time value to information—just as there is to money. Sometimes it is sufficient to protect a message for a few hours or days. Also, because security is costly, we always have to weigh the cost against the potential loss. Finally, we have also learned that security is a chain that breaks most often at the weakest link. Our locks are often much stronger than our management of the keys.

We can conclude then that good e-commerce security requires a set of laws, procedures, policies, and technologies that, to the extent feasible, protect individuals and organizations from unexpected behavior in the e-commerce marketplace.

DIMENSIONS OF E-COMMERCE SECURITY

There are six key dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability.

integrity
the ability to ensure that information being displayed on a website or transmitted or received over the Internet has not been altered in any way by an unauthorized party

Integrity refers to the ability to ensure that information being displayed on a website, or transmitted or received over the Internet, has not been altered in any way by an unauthorized party. For example, if an unauthorized person intercepts and changes the contents of an online communication, such as by redirecting a bank wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended.

nonrepudiation
the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions

Nonrepudiation refers to the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions. For instance, the availability of free e-mail accounts with alias names makes it easy for a person to post comments or send a message and perhaps later deny doing so. Even when a customer uses a real name and e-mail address, it is easy for that customer to order merchandise online and then later deny doing so. In most cases, because merchants typically do not obtain a physical copy of a signature, the credit card issuer will side with the customer because the merchant has no legally valid proof that the customer ordered the merchandise.

authenticity
the ability to identify the identity of a person or entity with whom you are dealing on the Internet

Authenticity refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet. How does the customer know that the website operator is who it claims to be? How can the merchant be assured that the customer is really who she says she is? Someone who claims to be someone he is not is "spoofing" or misrepresenting himself.

confidentiality
the ability to ensure that messages and data are available only to those who are authorized to view them

Confidentiality refers to the ability to ensure that messages and data are available only to those who are authorized to view them. Confidentiality is sometimes confused with **privacy**, which refers to the ability to control the use of information a customer provides about himself or herself to an e-commerce merchant.

privacy
the ability to control the use of information about oneself

E-commerce merchants have two concerns related to privacy. They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use. For example, if hackers break into an e-commerce site and gain access to credit card or other information, this violates not only the confidentiality of the data, but also the privacy of the individuals who supplied the information.

TABLE 5.3 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

availability
the ability to ensure that an e-commerce site continues to function as intended

Availability refers to the ability to ensure that an e-commerce site continues to function as intended.

Table 5.3 summarizes these dimensions from both the merchants' and customers' perspectives. E-commerce security is designed to protect these six dimensions. When any one of them is compromised, overall security suffers.

THE TENSION BETWEEN SECURITY AND OTHER VALUES

Can there be too much security? The answer is yes. Contrary to what some may believe, security is not an unmitigated good. Computer security adds overhead and expense to business operations, and also gives criminals new opportunities to hide their intentions and their crimes.

Ease of Use

There are inevitable tensions between security and ease of use. When traditional merchants are so fearful of robbers that they do business in shops locked behind security gates, ordinary customers are discouraged from walking in. The same can be true with respect to e-commerce. In general, the more security measures added to an

e-commerce site, the more difficult it is to use and the slower the site becomes. As you will discover reading this chapter, digital security is purchased at the price of slowing down processors and adding significantly to data storage demands on storage devices. Security is a technological and business overhead that can detract from doing business. Too much security can harm profitability, while not enough security can potentially put you out of business. One solution is to adjust security settings to the user's preferences. A recent McKinsey report found that when consumers find authentication at websites easy, they purchased 10% to 20% more. About 30% of the Internet population prioritizes ease of use and convenience over security, while 10% prioritize security. The report suggests it is possible to have both ease of use and security by adjusting the authentication process for each customer, providing options from automatic login (low security), to downloadable one-time passwords (high security) (Hasham, et al., 2016).

Public Safety and the Criminal Uses of the Internet

There is also an inevitable tension between the desires of individuals to act anonymously (to hide their identity) and the needs of public officials to maintain public safety that can be threatened by criminals or terrorists. This is not a new problem, or even new to the electronic era. The U.S. government began tapping telegraph wires during the Civil War in the mid-1860s in order to trap conspirators and terrorists, and the first police wiretaps of local telephone systems were in place by the 1890s—20 years after the invention of the phone (Schwartz, 2001). No nation-state has ever permitted a technological haven to exist where criminals can plan crimes or threaten the nation-state without fear of official surveillance or investigation. In this sense, the Internet is no different from any other communication system. Drug cartels make extensive use of voice, fax, the Internet, and encrypted e-mail; a number of large international organized crime groups steal information from commercial websites and resell it to other criminals who use it for financial fraud. Over the years, the U.S. government has successfully pursued various "carding forums" (websites that facilitate the sale of stolen credit card and debit card numbers), such as Shadowcrew, Carderplanet, and Cardersmarket, resulting in the arrest and prosecution of a number of their members and the closing of the sites. However, other criminal organizations have emerged to take their place.

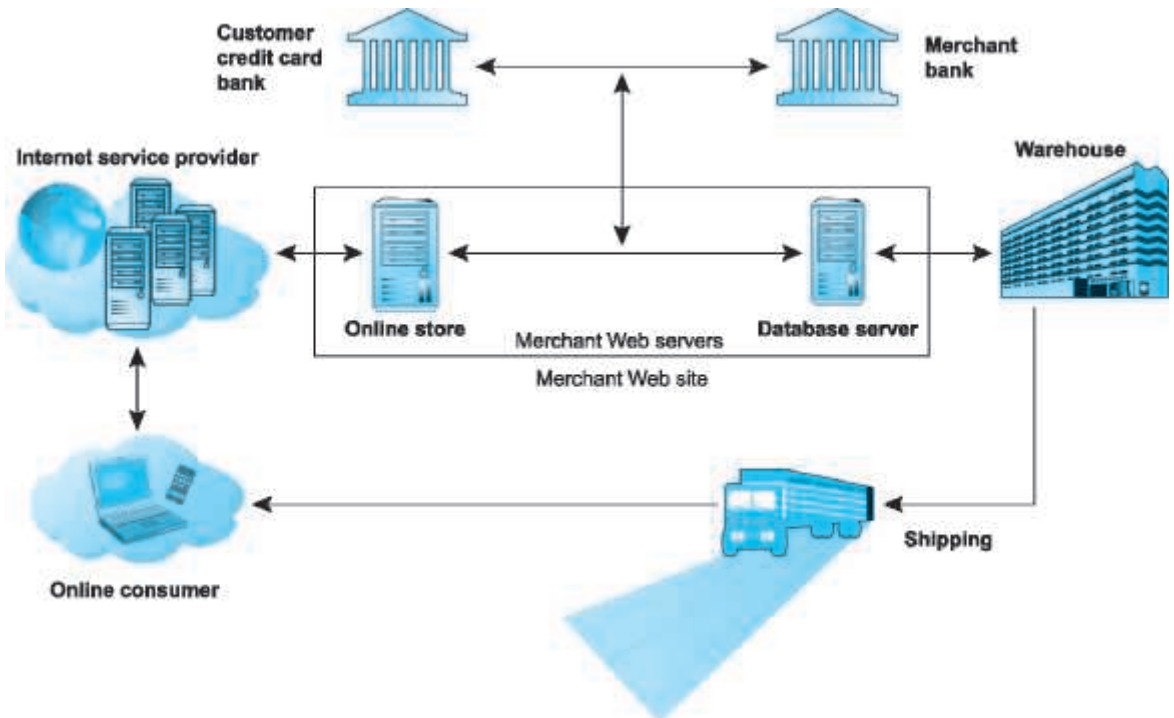
The Internet and mobile platform also provide terrorists with convenient communications channels. Encrypted files sent via e-mail were used by Ramzi Yousef—a member of the terrorist group responsible for bombing the World Trade Center in 1993—to hide plans for bombing 11 U.S. airliners. The Internet was also used to plan and coordinate the subsequent attacks on the World Trade Center on September 11, 2001. The case of Umar Farouk Abdulmutallab further illustrates how terrorists make effective use of the Internet to radicalize, recruit, train, and coordinate youthful terrorists. Abdulmutallab allegedly attempted to blow up an American airliner in Detroit on Christmas Day 2009. He was identified, contacted, recruited, and trained, all within six weeks, according to a Pentagon counterterrorism official. In an effort to combat such terrorism, the U.S. government has significantly ramped up its surveillance of communications delivered via the Internet over the past several years. The extent of that surveillance created a major controversy with National Security Agency contrac-

tor Edward Snowden's release of classified NSA documents that revealed that the NSA had obtained access to the servers of major Internet companies such as Facebook, Google, Apple, Microsoft, and others, as well as that NSA analysts have been searching e-mail, online chats, and browsing histories of U.S. citizens without any court approval. Security agencies have shifted from mass surveillance to smaller, targeted surveillance of terrorists and terrorist groups, and the use of predictive algorithms to focus their efforts (N.F. Johnson, et al., 2016). The proper balance between public safety and privacy in the effort against terrorism has proven to be a very thorny problem for the U.S. government.

5.2 SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT

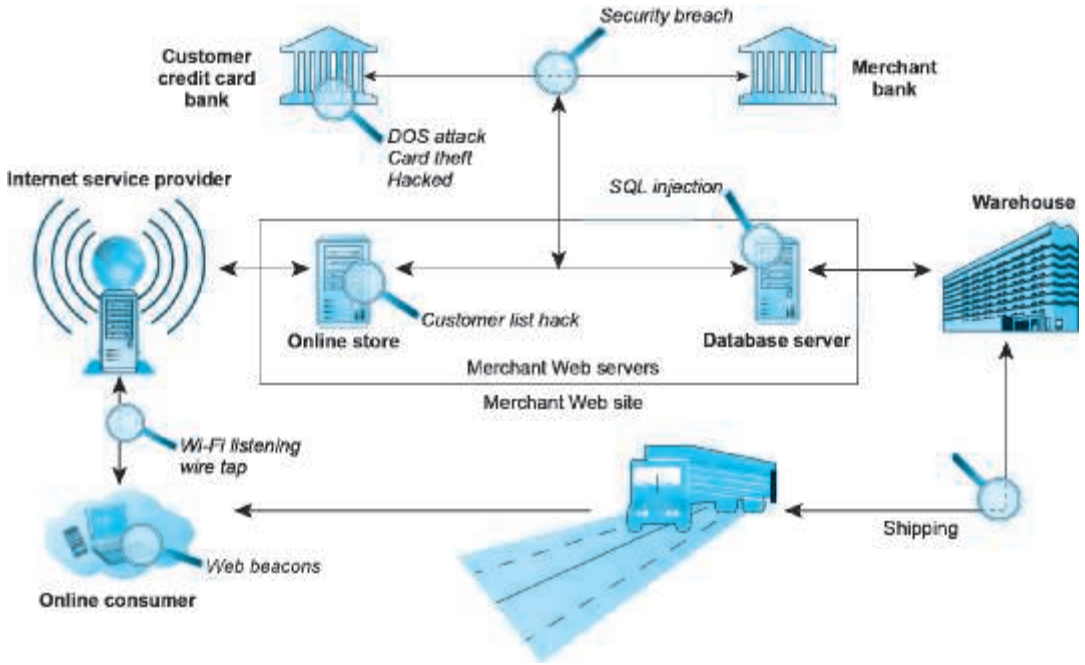
From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the client, the server, and the communications pipeline. **Figure 5.2** illustrates a typical e-commerce transaction with a consumer using a credit

FIGURE 5.2 A TYPICAL E-COMMERCE TRANSACTION



In a typical e-commerce transaction, the customer uses a credit card and the existing credit payment system.

FIGURE 5.3 VULNERABLE POINTS IN AN E-COMMERCE TRANSACTION



There are three major vulnerable points in e-commerce transactions: Internet communications, servers, and clients.

card to purchase a product. **Figure 5.3** illustrates some of the things that can go wrong at each major vulnerability point in the transaction—over Internet communications channels, at the server level, and at the client level.

In this section, we describe a number of the most common and most damaging forms of security threats to e-commerce consumers and site operators: malicious code, potentially unwanted programs, phishing, hacking and cybervandalism, credit card fraud/theft, spoofing, pharming, spam (junk) websites (link farms), identity fraud, Denial of Service (DoS) and DDoS attacks, sniffing, insider attacks, poorly designed server and client software, social network security issues, mobile platform security issues, and finally, cloud security issues.

MALICIOUS CODE

Malicious code (sometimes referred to as "malware") includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots. Some malicious code, sometimes referred to as an *exploit,* is designed to take advantage of software vulnerabilities in a computer's operating system, web browser, applications, or other software components. **Exploit kits** are collections of exploits bundled together and rented or sold as a commercial product, often with slick user interfaces and in-depth analytics functionality. Use of an exploit kit typically does not require much technical skill, enabling novices

malicious code (malware)
includes a variety of threats such as viruses, worms, Trojan horses, and bots

exploit kit
collection of exploits bundled together and rented or sold as a commercial product

to become cybercriminals. Exploit kits typically target software that is widely deployed, such as Microsoft Windows, Internet Explorer, Adobe Flash and Reader, and Oracle Java. In 2014, according to Cisco, Angler, an exploit kit that uses Flash, Java, Microsoft Internet Explorer, and Microsoft Silverlight vulnerabilities, was one of the exploit kits most observed "in the wild" (Cisco, 2016). According to Symantec, more than 430 million new variants of malware were created in 2015, an average of more than a million strains a day, up 36% in one year (Symantec, 2016). In the past, malicious code was often intended to simply impair computers, and was often authored by a lone hacker, but increasingly it involves a small group of hackers or a nation-state supported group, and the intent is to steal e-mail addresses, logon credentials, personal data, and financial information. It's the difference between petty crime and organized crime.

Malware is often delivered in the form of a malicious attachment to an email or embedded as a link in the email. Malicious links can also be placed in innocent-looking Microsoft Word or Excel documents. The links lead directly to a malicious code download or websites that include malicious code (Symantec, 2016). One of the latest innovations in malicious code distribution is to embed it in the online advertising chain (known as **maladvertising**), including in Google, AOL, and other ad networks (Goodin, 2016). As the ad network chain becomes more complicated, it becomes more and more difficult for websites to vet ads placed on their sites to ensure they are malware-free. A 2014 research study indicated that as many as 1% of all ads served may be maladvertising (Zarras et al., 2014). The largest advertising malware infection occurred at Yahoo where more than 6.9 million daily visitors were exposed to malicious pop-up ads (Blue, 2016). These malicious ads can be stopped by turning on pop-up blockers in users' browsers. Much of the maladvertising in the recent years has been in the form of drive-by downloads that exploited the frequent zero-day vulnerabilities that have plagued Adobe Flash, which is often used for online advertisements. As a result, the Internet Advertising Bureau has urged advertisers to abandon Adobe Flash in favor of HTML5, and Mozilla Firefox, Apple's Safari, and Google's Chrome browser all now block Flash advertisements from autoplaying. Amazon has also stopped accepting Flash ads (see the Chapter 3 *Insight on Technology* case, *The Rise of HTML5*). A **drive-by download** is malware that comes with a downloaded file that a user intentionally or unintentionally requests. Drive-by is now one of the most common methods of infecting computers. For instance, websites as disparate as the New York Times, MSN, Yahoo, and AOL have experienced instances where ads placed on their sites either had malicious code embedded or directed clickers to malicious sites. According to Symantec, drive-by download exploit kits, including updates and 24/7 support, can be rented for between $100 to $700 per week. Malicious code embedded in PDF files also is common. Equally important, there has been a major shift in the writers of malware from amateur hackers and adventurers to organized criminal efforts to defraud companies and individuals. In other words, it's now more about the money than ever before.

maladvertising
online advertising that contains malicious code

drive-by download
malware that comes with a downloaded file that a user requests

A **virus** is a computer program that has the ability to replicate or make copies of itself, and spread to other files. In addition to the ability to replicate, most computer viruses deliver a "payload." The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive—destroying files, reformatting the computer's hard drive, or causing programs to run improperly.

virus
a computer program that has the ability to replicate or make copies of itself, and spread to other files

Viruses are often combined with a worm. Instead of just spreading from file to file, a **worm** is designed to spread from computer to computer. A worm does not necessarily need to be activated by a user or program in order for it to replicate itself. The Slammer worm is one of the most notorious. Slammer targeted a known vulnerability in Microsoft's SQL Server database software and infected more than 90% of vulnerable computers worldwide within 10 minutes of its release on the Internet; crashed Bank of America cash machines, especially in the southwestern part of the United States; affected cash registers at supermarkets such as the Publix chain in Atlanta, where staff could not dispense cash to frustrated buyers; and took down most Internet connections in South Korea, causing a dip in the stock market there. The Conficker worm, which first appeared in November 2008, is the most significant worm since Slammer, and reportedly infected 11 million computers worldwide (Microsoft, 2015). Originally designed to establish a global botnet, a massive industry effort has defeated this effort, but Conficker still resides on over 800,000 Internet devices in 2016. It is the most widely detected malware on the Internet.

worm
malware that is designed to spread from computer to computer

Ransomware (scareware) is a type of malware (often a worm) that locks your computer or files to stop you from accessing them. Ransomware will often display a notice that says an authority such as the FBI, Department of Justice, or IRS has detected illegal activity on your computer and demands that you pay a fine in order to unlock the computer and avoid prosecution. One type of ransomware is named CryptoLocker. CryptoLocker encrypts victims' files with a virtually unbreakable asymmetric encryption and demands a ransom to decrypt them, often in Bitcoins. If the victim does not comply within the time allowed, the files will not ever be able to be decrypted. Other variants include CryptoDefense and Cryptowall. Ransomware attacks increased by over 400% in 2016, and the U.S. Department of Justice reports that there are over 4,000 ransomware attacks daily, up from 1,000 daily in 2015 (U.S. Department of Justice, 2016). Crypto-ransomware infections often take place via a malicious e-mail attachment that purports to be an invoice (Symantec, 2016). The growth of ransomware is also related to the growth of the virtual currency Bitcoin. Hackers often demand victims pay using Bitcoin so their transactions are hidden from authorities (McMillan, 2016).

ransomware (scareware)
malware that prevents you from accessing your computer or files and demands that you pay a fine

A **Trojan horse** appears to be benign, but then does something other than expected. The Trojan horse is not itself a virus because it does not replicate, but is often a way for viruses or other malicious code such as bots or *rootkits* (a program whose aim is to subvert control of the computer's operating system) to be introduced into a computer system. The term *Trojan horse* refers to the huge wooden horse in Homer's *Iliad* that the Greeks gave their opponents, the Trojans—a gift that actually contained hundreds of Greek soldiers. Once the people of Troy let the massive horse within their gates, the soldiers revealed themselves and captured the city. In today's world, a Trojan horse may masquerade as a game, but actually hide a program to steal your passwords and e-mail them to another person. Miscellaneous Trojans and Trojan downloaders and droppers (Trojans that install malicious files to a computer they have infected by either downloading them from a remote computer or from a copy contained in their own code) are a common type of malware. According to Panda Security, Trojans accounted for over 50% of all malware created in 2015, and over 60% of all malware infections (Panda Security, 2016). In 2011, Sony experienced the largest data

Trojan horse
appears to be benign, but then does something other than expected. Often a way for viruses or other malicious code to be introduced into a computer system

breach in history up to that time when a Trojan horse took over the administrative computers of Sony's PlayStation game center and downloaded personal and credit card information involving 77 million registered users (Wakabayashi, 2011). Trojan horses are often used for financial malware distributed via botnets. One example is Zeus, which steals information by keystroke logging and has infected over 10 million computers since it first became known in 2007. Other examples include SpyEye, a Trojan that can steal banking information via both a keylogging application and the ability to take screenshots on a victim's computer; Torpig, a botnet that is spread by a Trojan horse called Meboot; and Vawtrak, a Trojan that spreads via social media, e-mail, and FTP, and is able to hide evidence of fraud by changing bank balances shown to the victim on the fly (Cyphort, 2015).

backdoor
feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer

A **backdoor** is a feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer. Downadup is an example of a worm with a backdoor, while Virut, a virus that infects various file types, also includes a backdoor that can be used to download and install additional threats.

bot
type of malicious code that can be covertly installed on a computer when connected to the Internet. Once installed, the bot responds to external commands sent by the attacker

botnet
collection of captured bot computers

Bots (short for robots) are a type of malicious code that can be covertly installed on your computer when attached to the Internet. Once installed, the bot responds to external commands sent by the attacker; your computer becomes a "zombie" and is able to be controlled by an external third party (the "bot-herder"). **Botnets** are collections of captured computers used for malicious activities such as sending spam, participating in a DDoS attack, stealing information from computers, and storing network traffic for later analysis. The number of botnets operating worldwide is not known but is estimated to be well into the thousands, controlling millions of computers. Bots and bot networks are an important threat to the Internet and e-commerce because they can be used to launch very large-scale attacks using many different techniques. In 2011, federal marshals accompanied members of Microsoft's digital crimes unit in raids designed to disable the Rustock botnet, at that time the leading source of spam in the world with nearly 500,000 slave PCs under the control of its command and control servers located at six Internet hosting services in the United States. Officials confiscated the Rustock control servers at the hosting sites, which claimed they had no idea what the Rustock servers were doing. The actual spam e-mails were sent by the slave PCs under the command of the Rustock servers (Wingfield, 2011). In 2013, Microsoft and the FBI engaged in another aggressive botnet operation, targeting 1,400 of Zeus-derived Citadel botnets, which had been used in 2012 to raid bank accounts at major banks around the world, netting over $500 million (Chirgwin, 2013). In April 2015, an international cybersquad took down the Beebone botnet, made up of 12,000 computers that had been infecting about 30,000 computers a month around the world via drive-by downloads with Changeup, a polymorphic worm used to distribute Trojans, worms, backdoors, and other types of malware (Constantin, 2015). In 2015, the FBI and British police were also able to stop a botnet that had stolen over $10 million from banks (Pagliery, 2015). As a result of efforts such as these, the number of bots has significantly declined, especially in the United States (Symantec, 2016).

Malicious code is a threat at both the client and the server levels, although servers generally engage in much more thorough anti-virus activities than do consumers. At

TABLE 5.4 NOTABLE EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Cryptolocker	Ransomware/ Trojan	Hijacks users' photos, videos, and text documents, encrypts them with virtually unbreakable asymmetric encryption, and demands ransom payment for them.
Citadel	Trojan/botnet	Variant of Zeus Trojan, focuses on the theft of authentication credentials and financial fraud. Botnets spreading Citadel were targets of Microsoft/FBI action in 2012.
Zeus	Trojan/botnet	Sometimes referred to as king of financial malware. May install via drive-by download and evades detection by taking control of web browser and stealing data that is exchanged with bank servers.
Reveton	Ransomware worm/Trojan	Based on Citadel/Zeus Trojans. Locks computer and displays warning from local police alleging illegal activity on computer; demands payment of fine to unlock.
Ramnit	Virus/worm	One of the most prevalent malicious code families still active in 2013. Infects various file types, including executable files, and copies itself to removable drives, executing via AutoPlay when the drive is accessed on other computers
Sality.AE	Virus/worm	Most common virus in 2012; still active in 2013. Disables security applications and services, connects to a botnet, then downloads and installs additional threats. Uses polymorphism to evade detection.
Conficker	Worm	First appeared November 2008. Targets Microsoft operating systems. Uses advanced malware techniques. Largest worm infection since Slammer in 2003. Still considered a major threat.
Netsky.P	Worm/Trojan	First appeared in early 2003. It spreads by gathering target e-mail addresses from the computers, then infects and sends e-mail to all recipients from the infected computer. It is commonly used by bot networks to launch spam and DoS attacks.
Storm (Peacomm, NuWar)	Worm/Trojan	First appeared in January 2007. It spreads in a manner similar to the Netsky.P worm. May also download and run other Trojan programs and worms.
Nymex	Worm	First discovered in January 2006. Spreads by mass mailing; activates on the 3rd of every month, and attempts to destroy files of certain types.
Zotob	Worm	First appeared in August 2005. Well-known worm that infected a number of U.S. media companies.
Mydoom	Worm	First appeared in January 2004. One of the fastest spreading mass-mailer worms.
Slammer	Worm	Launched in January 2003. Caused widespread problems.
CodeRed	Worm	Appeared in 2001. It achieved an infection rate of over 20,000 systems within 10 minutes of release and ultimately spread to hundreds of thousands of systems.
Melissa	Macro virus/ worm	First spotted in March 1999. At the time, the fastest spreading infectious program ever discovered. It attacked Microsoft Word's Normal.dot global template, ensuring infection of all newly created documents. It also mailed an infected Word file to the first 50 entries in each user's Microsoft Outlook Address Book.
Chernobyl	File-infecting virus	First appeared in 1998. It wipes out the first megabyte of data on a hard disk (making the rest useless) every April 26, the anniversary of the nuclear disaster at Chernobyl.

the server level, malicious code can bring down an entire website, preventing millions of people from using the site. Such incidents are infrequent. Much more frequent malicious code attacks occur at the client level, and the damage can quickly spread to millions of other computers connected to the Internet. **Table 5.4** lists some well-known examples of malicious code.

POTENTIALLY UNWANTED PROGRAMS (PUPS)

potentially unwanted program (PUP)
program that installs itself on a computer, typically without the user's informed consent

In addition to malicious code, the e-commerce security environment is further challenged by **potentially unwanted programs (PUPs)** such as adware, browser parasites, spyware, and other applications that install themselves on a computer, such as rogue security software, toolbars, and PC diagnostic tools, typically without the user's informed consent. Such programs are increasingly found on social network and user-generated content sites where users are fooled into downloading them. Once installed, these applications are usually exceedingly difficult to remove from the computer. One example of a PUP is System Doctor, which infects PCs running Windows operating systems. System Doctor poses as a legitimate anti-spyware program when in fact it is malware that, when installed, disables the user's security software, alters the user's web browser, and diverts users to scam websites where more malware is downloaded.

adware
a PUP that serves pop-up ads to your computer

browser parasite
a program that can monitor and change the settings of a user's browser

Adware is typically used to call for pop-up ads to display when the user visits certain sites. While annoying, adware is not typically used for criminal activities. A **browser parasite** is a program that can monitor and change the settings of a user's browser, for instance, changing the browser's home page, or sending information about the sites visited to a remote computer. Browser parasites are often a component of adware. In early 2015, Lenovo faced a barrage of criticism when it became known that, since September 2014, it had been shipping its Windows laptops with Superfish adware preinstalled. Superfish injected its own shopping results into the computer's browser when the user searched on Google, Amazon, or other websites. In the process, Superfish created a security risk by enabling others on a Wi-Fi network to silently hijack the browser and collect anything typed into it. Lenovo ultimately issued a removal tool to enable customers to delete the adware. Microsoft and legitimate security firms have redefined adware programs to be malware and discourage manufacturers from shipping products with adware programs (Loeb, 2016).

spyware
a program used to obtain information such as a user's keystrokes, e-mail, instant messages, and so on

Spyware, on the other hand, can be used to obtain information such as a user's keystrokes, copies of e-mail and instant messages, and even take screenshots (and thereby capture passwords or other confidential data).

PHISHING

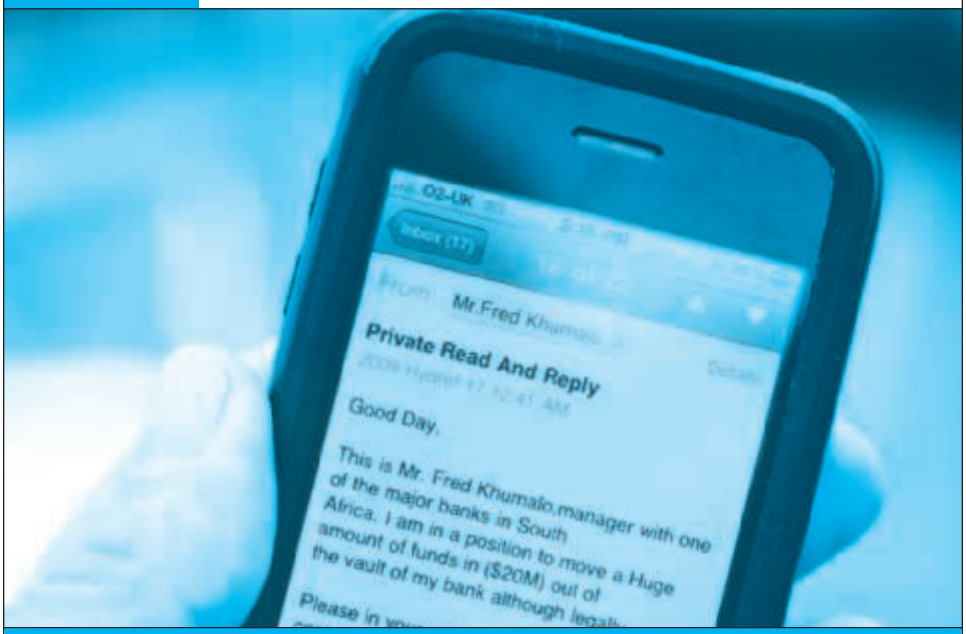
social engineering
exploitation of human fallibility and gullibility to distribute malware

Social engineering relies on human curiosity, greed, and gullibility in order to trick people into taking an action that will result in the downloading of malware. Kevin Mitnick, until his capture and imprisonment in 1999, was one of America's most wanted computer criminals. Mitnick used simple deceptive techniques to obtain passwords, social security, and police records all without the use of any sophisticated technology (Mitnick, 2011).

phishing
any deceptive, online attempt by a third party to obtain confidential information for financial gain

Phishing is any deceptive, online attempt by a third party to obtain confidential information for financial gain. Phishing attacks typically do not involve malicious code but instead rely on straightforward misrepresentation and fraud, so-called "social engineering" techniques. One of the most popular phishing attacks is the e-mail scam letter. The scam begins with an e-mail: a rich former oil minister of Nigeria is seeking a bank account to stash millions of dollars for a short period of time, and requests your bank account number where the money can be deposited. In return, you will receive

FIGURE 5.4 AN EXAMPLE OF A NIGERIAN LETTER E-MAIL SCAM



This is an example of a typical Nigerian letter e-mail scam.
© keith morris / Alamy

a million dollars. This type of e-mail scam is popularly known as a "Nigerian letter" scam (see **Figure 5.4**).

Thousands of other phishing attacks use other scams, some pretending to be eBay, PayPal, or Citibank writing to you for account verification (known as *spear phishing,* or targeting a known customer of a specific bank or other type of business). Click on a link in the e-mail and you will be taken to a website controlled by the scammer, and prompted to enter confidential information about your accounts, such as your account number and PIN codes. On any given day, millions of these phishing attack e-mails are sent, and, unfortunately, some people are fooled and disclose their personal account information.

Phishers rely on traditional "con man" tactics, but use e-mail to trick recipients into voluntarily giving up financial access codes, bank account numbers, credit card numbers, and other personal information. Often, phishers create (or "spoof") a website that purports to be a legitimate financial institution and cons users into entering financial information, or the site downloads malware such as a keylogger to the victim's computer. Phishers use the information they gather to commit fraudulent acts such as charging items to your credit cards or withdrawing funds from your bank account, or in other ways "steal your identity" (identity fraud). Symantec reported that in 2015, about 1 in every 1,875 e-mails contained a phishing attack. The number of spear-phishing campaigns in 2015 increased by 55%, but the number of attacks, recipients within each campaign, and the average duration of the campaign all declined, indi-

cating that perpetrators are becoming stealthier about them, since campaigns that target fewer recipients and are smaller and shorter are less likely to arouse suspicion. In 2015, according to Symantec, 43% of spear-phishing e-mails were directed at small businesses with less than 250 employees, and 35% of large organizations reported they were targeted in spear-phishing campaigns (Symantec, 2016). According to Verizon, 30% of phishing emails were opened by their targets, and 12% were clicked on to open attachments (Verizon, 2016).

To combat phishing, in January 2012, leading e-mail service providers, including Google, Microsoft, Yahoo, and AOL, as well as financial services companies such as PayPal, Bank of America, and others, joined together to form DMARC.org, an organization aimed at dramatically reducing e-mail address spoofing, in which attackers use real e-mail addresses to send phishing e-mails to victims who may be deceived because the e-mail appears to originate from a source the receiver trusts. DMARC offers a method of authenticating the origin of the e-mail and allows receivers to quarantine, report, or reject messages that fall to pass its test. Yahoo and AOL have reported significant success against email fraud as a result of using DMARC, and, effective as of June 2016, Google joined them in implementing a stricter version of DMARC, in which e-mail that fails DMARC authentication checks will be rejected (Vijayan, 2015).

HACKING, CYBERVANDALISM, AND HACKTIVISM

hacker
an individual who intends to gain unauthorized access to a computer system

cracker
within the hacking community, a term typically used to denote a hacker with criminal intent

cybervandalism
intentionally disrupting, defacing, or even destroying a site

hacktivism
cybervandalism and data theft for political purposes

A **hacker** is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term **cracker** is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker tend to be used interchangeably. Hackers and crackers gain unauthorized access by finding weaknesses in the security procedures of websites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use. In the past, hackers and crackers typically were computer aficionados excited by the challenge of breaking into corporate and government websites. Sometimes they were satisfied merely by breaking into the files of an e-commerce site. Today, hackers have malicious intentions to disrupt, deface, or destroy sites (**cybervandalism**) or to steal personal or corporate information they can use for financial gain (data breach).

Hacktivism adds a political twist. Hacktivists typically attack governments, organizations, and even individuals for political purposes, employing the tactics of cybervandalism, distributed denial of service attacks, data thefts, and doxing (gathering and exposing personal information of public figures, typically from emails, social network posts, and other documents). The most prominent hacktivist organization is Wikileaks, founded by Julian Assange and others, which released documents and e-mails of the U.S. Department of State, U.S. Department of Defense, and Democratic National Committee in 2016. LulzSec and Anonymous are two other prominent hacktivist groups. In 2015, another hacktivist group called the Impact Team allegedly hacked the Ashley Madison website to call attention to its weak security, and after its owner Avid Life Media refused to shut it down as they demanded, the group released millions of sensitive customer records. See the *Insight on Society* case study, *The Ashley Madison Data Breach*, for a more in-depth look at implications of this high-profile hack.

INSIGHT ON SOCIETY

THE ASHLEY MADISON DATA BREACH

As the Internet continues to permeate even the most intimate aspects of our lives, the stigma attached to online dating has largely disappeared. Online dating has grown into a $2.2 billion industry annually in the United States, led by companies like eHarmony, OKCupid, and Match. There are also a number of smaller niche sites that cater to people with more specific interests or lifestyles. One such site is Ashley Madison.

Based in Canada and launched in 2001 by its parent company, Avid Life Media, Ashley Madison specifically markets itself to people in marriages or committed relationships, which has earned the site a tawdry reputation. Users purchase credits, rather than a monthly subscription, and then redeem the credits to participate in conversations with other members, which can be through messages or real-time chat. Women are not charged money to create a profile on the site, nor are they charged to send or receive messages, while men are charged for both. Even with those incentives, the ratio of men to women on the site skews dramatically toward men, which led Ashley Madison to create fictitious female profiles to create the appearance of balance.

The perception of secrecy is critical for prospective users of Ashley Madison. But in 2015, that veil of secrecy came crashing down. The site was hacked by a group known as The Impact Team, which stated that its motivations were to harm the site and its unethical business model, as well as to protest the site's use of a $19 data deletion fee for users seeking to close their accounts. The Impact Team stated that after creating a plan to make an undetectable breach, they discovered they were easily able to access the entire cache of company data. They released the data in two batches of 10 and 12 gigabytes, and the data is now easily searchable on the Web. Names, street addresses, and dates of birth were all stolen and made public, as well as other personal information. They also stole company documents, including the e-mails of CEO Noel Biderman, many of which caused further damage to the company's shattered reputation. For example, Biderman's e-mails revealed that the CTO of Ashley Madison had hacked a competitor's database, revealing key security flaws (perhaps he should have been paying more attention to his own company's security systems). Partial credit card information of Ashley Madison users was also leaked, but not enough for identity thieves to use.

Demographic information gleaned from the data dump shows that of the site's 36 million users, 31 million were males, but only 10 million actively used the site. The other 5 million profiles were female, but less than 2,500 of those were involved in chats with other users, suggesting that fake female profiles were the overwhelming majority of female profiles on the site. A full third of the accounts on the site were created with dummy e-mail addresses. North Americans had the highest number of accounts as a percentage of population, with the United States coming in at 5.1%. E-mail addresses associated with government accounts were well-represented, as were big banks, large tech companies, and other high-powered industries. This stands in stark demographic contrast to a service like Tinder, which consists of much younger members; Ashley Madison users tended to be more established financially and willing to pay for what they perceived to be a discreet and upscale service. After the hack, researchers found that companies with a disproportionately high number of Ashley Madison members took bigger financial risks and had poor scores in corporate responsibility.

Ashley Madison's own corporate profile suggests risk-taking of its own. How could a site

(continued)

that advertises the ability to discreetly have an affair allow its data to be breached and stolen so easily? Security experts reviewing Ashley Madison's setup claimed that the site lacked even simplistic security measures. For example, all of the data belonging to users who paid the $19 data deletion fee persisted on Ashley Madison servers and was obtained in the hack. Additionally, none of the data was encrypted. Encryption would have incurred hefty additional expense for the company, but it might have saved it considerable embarrassment during a breach like this one.

Most data breaches allow criminals to engage in identity theft and other types of online fraud. But in this case, the Ashley Madison hack has even more significant ramifications on the personal lives of its users. There are already multiple reported incidents of suicides committed by former users, and a handful of notable public figures have been publicly embarrassed by the release of their profile data. The hack has the potential to ruin the marriages and personal lives of thousands of people. Although many of Ashley Madison's users were engaged in infidelity, these people were still the victims of a crime and an invasion of privacy that goes beyond typical data breaches. Spammers and blackmailers have used the now-public data to extort users, demanding Bitcoin in exchange for silence and threatening to share Ashley Madison data with users' families and social media contacts.

As a result of the hack, Biderman quickly stepped down from his post as CEO, and in 2016 a new executive team was installed and immediately began distancing themselves from the previous regime. Going forward, the revelations about fake profiles, impending lawsuits, and overall negative coverage of the breach will likely derail plans for growth. Ashley Madison had already struggled to market its business and raise funds in the past, despite its very solid financial profile. The company had been growing so fast that Biderman had started investigating launching an IPO in England to fuel its expansion. Not only are those plans on hold indefinitely, but the Federal Trade Commission has begun investigating Ashley Madison's usage of bots and other fake profiles. Ashley Madison has also begun to receive what may become a barrage of lawsuits alleging negligence and personal damages, though many potential plaintiffs may be unwilling to reveal their identities, which they must do to be included in any suit after a judge ruled in 2016 that plaintiffs could not use aliases such as John Doe. And the results of a joint investigation by the Canadian and Australian governments completed in 2016 confirmed that the company had fabricated a "trusted security award" displayed on its homepage. The investigation also confirmed the company's failure to delete profile information of users who canceled their accounts.

Despite the turmoil, the company estimates that its membership base has actually grown over the past year. However, a third-party analysis showed that traffic to the site has dropped by 82% since the breach, calling the site's self-reported numbers into question.

SOURCES: "Ashley Madison Blasted Over Fake Security Award as Lawsuit Moves Forward," by Jeff John Roberts, *Fortune*, August 25, 2016; "You Blew It, Ashley Madison: Dating Site Slammed for Security 'Shortcomings,'" by Claire Reilly Cnet.com, August 23, 2015; "Ashley Madison Parent, Under FTC Investigation, Launches Turnaround Plans," by Maria Armental and Austen Hufford, *Wall Street Journal*, July 5, 2016; "Infidelity Website Ashley Madison Facing FTC Probe, Apologizes," Alastair Sharp and Allison Martell, by Reuters.com, July 5, 2016; "Ashley Madison Hacking Victims Face Big Decision," by Robert Hackett, *Fortune*, April 20, 2016; "The Ashley Madison Effect on Companies," by Justin Lahart, *Wall Street Journal,* March 6, 2016; "Life After the Ashley Madison Affair," by Tom Lamont, Theguardian.com, February 27, 2016; "It's Been Six Months Since the Ashley Madison Hack. Has Anything Changed?" by Caitlin Dewey, *Washington Post,* January 15, 2016; "Ashley Madison Hack Victims Receive Blackmail Letters," BBC, December 15, 2015; "Ashley Madison Hack: 6 Charts That Show Who Uses the Infidelity Website," by Zachary Davies Boren, Independent.co.uk, August 21, 2015; "Ashley Madison Hackers Speak Out: 'Nobody Was Watching', by Joseph Cox, Motherboard.vice.com, August 21, 2015; "The Ashley Madison Hack, Explained," by Timothy B. Lee, Vox.com, August 19, 2015; "Who Is Ashley Madison," by Paul R. LaMonica, CNN Money, July 20, 2015.

Groups of hackers called *tiger teams* are sometimes used by corporate security departments to test their own security measures. By hiring hackers to break into the system from the outside, the company can identify weaknesses in the computer system's armor. These "good hackers" became known as **white hats** because of their role in helping organizations locate and fix security flaws. White hats do their work under contract, with agreement from the target firms that they will not be prosecuted for their efforts to break in. Hardware and software firms such as Apple and Microsoft pay bounties of $25,000 to $200,000 to white hat hackers for discovering bugs in their software and hardware (Perlroth, 2016).

white hats
"good" hackers who help organizations locate and fix security flaws

In contrast, **black hats** are hackers who engage in the same kinds of activities but without pay or any buy-in from the targeted organization, and with the intention of causing harm. They break into websites and reveal the confidential or proprietary information they find. These hackers believe strongly that information should be free, so sharing previously secret information is part of their mission.

black hats
hackers who act with the intention of causing harm

Somewhere in the middle are the **grey hats**, hackers who believe they are pursuing some greater good by breaking in and revealing system flaws. Grey hats discover weaknesses in a system's security, and then publish the weakness without disrupting the site or attempting to profit from their finds. Their only reward is the prestige of discovering the weakness. Grey hat actions are suspect, however, especially when the hackers reveal security flaws that make it easier for other criminals to gain access to a system.

grey hats
hackers who believe they are pursuing some greater good by breaking in and revealing system flaws

DATA BREACHES

A **data breach** occurs whenever organizations lose control over corporate information to outsiders. According to Symantec, the total number of data breaches in 2015 grew by only 2% compared to 2014, which was a record year for breaches. There were nine mega-breaches in 2015, up from eight in 2014. The total identities exposed reached 429 million, up 23%, with over 190 million identities exposed in a single breach (Symantec, 2016). The Identity Theft Resource Center is another organization that tracks data breaches. It recorded 780 breaches in 2015, the second highest total on record. Breaches involving the medical/healthcare industry had the highest impact, representing 35% of all breaches and almost 70% of all records exposed. Hackers were the leading cause of data breaches, responsible for almost 40% of breaches, followed by employee error/negligence (15%), accidental e-mail/Internet exposure (14%) and insider theft (11%). The number of breaches involving social security numbers involved almost 165 million people (Identity Theft Resource Center, 2016). Among the high profile breaches that occurred in 2015 were those affecting the Office of Personnel Management and the Internal Revenue Service, as well as others against health-care insurers such as Anthem and Premera, retailers such as CVS and Walgreens, and the credit rating agency Experian. In 2016, the trend has continued with the Yahoo data breach, which is believed to be the largest breach at a single company in history, exposing the records of 500 million. Compared to others like Google and Microsoft, Yahoo management was reportedly slow to invest in security measures (Perlroth and Goel, 2016).

data breach
occurs when an organization loses control over its information to outsiders

CREDIT CARD FRAUD/THEFT

Theft of credit card data is one of the most feared occurrences on the Internet. Fear that credit card information will be stolen prevents users from making online purchases in many cases. Interestingly, this fear appears to be largely unfounded. Incidences of stolen credit card information are actually much lower than users think, around 0.8% of all online card transactions (CyberSource, 2016). Online merchants use a variety of techniques to combat credit card fraud, including using automated fraud detection tools, manually reviewing orders, rejection of suspect orders, and requiring additional levels of security such as email address, zip code, and CCV security codes.

In addition, federal law limits the liability of individuals to $50 for a stolen credit card. For amounts more than $50, the credit card company generally pays the amount, although in some cases, the merchant may be held liable if it failed to verify the account or consult published lists of invalid cards. Banks recoup the cost of credit card fraud by charging higher interest rates on unpaid balances, and by merchants who raise prices to cover the losses. In 2016, the U.S. credit card system is in the midst of a shift to EMV credit cards, also known as smart cards or chip cards. Already widely used in Europe, EMV credit cards have a computer chip instead of a magnetic strip that can be easily copied by hackers and sold as dump data (see Table 5.2). While EMV technology cannot prevent data breaches from occurring, the hope is that it will make it harder for criminals to profit from the mass theft of credit card numbers that could be used in commerce.

In the past, the most common cause of credit card fraud was a lost or stolen card that was used by someone else, followed by employee theft of customer numbers and stolen identities (criminals applying for credit cards using false identities). Today, the most frequent cause of stolen cards and card information is the systematic hacking and looting of a corporate server where the information on millions of credit card purchases is stored. For instance, in 2010, Albert Gonzalez was sentenced to 20 years in prison for organizing one of the largest thefts of credit card numbers in American history. Along with several Russian co-conspirators, Gonzalez broke into the central computer systems of TJX, BJ's, Barnes & Noble, and other companies, stealing over 160 million card numbers and costing these firms over $200 million in losses (Fox and Botelho, 2013).

International orders have a much higher risk of being fraudulent, with fraud losses twice those of domestic orders. If an international customer places an order and then later disputes it, online merchants often have no way to verify that the package was actually delivered and that the credit card holder is the person who placed the order. As a result, most online merchants will not process international orders.

A central security issue of e-commerce is the difficulty of establishing the customer's identity. Currently there is no technology that can identify a person with absolute certainty. For instance, a lost or stolen EMV card can be used until the card is cancelled, just like a magnetic strip card. Until a customer's identity can be guaranteed, online companies are at a higher risk of loss than traditional offline companies. The federal government has attempted to address this issue through the Electronic Signatures in Global and National Commerce Act (the "E-Sign" law), which gives digital

signatures the same authority as hand-written signatures in commerce. This law also intended to make digital signatures more commonplace and easier to use. Although the use of e-signatures is still uncommon in the B2C retail e-commerce arena, many businesses are starting to implement e-signature solutions, particularly for B2B contracting, financial services, insurance, health care, and government and professional services. DocuSign, Adobe eSign, RightSignature, and Silanis eSignLive are currently among the most widely adopted e-signature solutions. They use a variety of techniques, such as remote user identification through third-party databases or personal information verification such as a photo of a driver's license; multi-factor user authentication methods (user ID and password, e-mail address verification, secret question and answer); and public/private key encryption to create a digital signature and embedded audit trail that can be used to verify the e-signature's integrity (Silanis Technology, 2014). The use of fingerprint identification is also one solution to positive identification, but the database of print information can be hacked. Mobile e-signature solutions are also beginning to be adopted (DocuSign, 2015).

IDENTITY FRAUD

Identity fraud involves the unauthorized use of another person's personal data, such as social security, driver's license, and/or credit card numbers, as well as user names and passwords, for illegal financial benefit. Criminals can use such data to obtain loans, purchase merchandise, or obtain other services, such as mobile phone or other utility services. Cybercriminals employ many of the techniques described previously, such as spyware, phishing, data breaches, and credit card theft, for the purpose of identity fraud. Data breaches, in particular, often lead to identity fraud.

identity fraud
involves the unauthorized use of another person's personal data for illegal financial benefit

Identity fraud is a significant problem in the United States. In 2015, according to Javelin Strategy & Research, 13 million U.S. consumers suffered identity fraud. The total dollar losses as a result of identity fraud were approximately $15 billion (Javelin Research & Strategy, 2016).

SPOOFING, PHARMING, AND SPAM (JUNK) WEBSITES

Spoofing involves attempting to hide a true identity by using someone else's e-mail or IP address. For instance, a spoofed e-mail will have a forged sender e-mail address designed to mislead the receiver about who sent the e-mail. IP spoofing involves the creation of TCP/IP packets that use someone else's source IP address, indicating that the packets are coming from a trusted host. Most current routers and firewalls can offer protection against IP spoofing. Spoofing a website sometimes involves **pharming**, automatically redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination. Links that are designed to lead to one site can be reset to send users to a totally unrelated site—one that benefits the hacker.

spoofing
involves attempting to hide a true identity by using someone else's e-mail or IP address

pharming
automatically redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination

Although spoofing and pharming do not directly damage files or network servers, they threaten the integrity of a site. For example, if hackers redirect customers to a fake website that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business from the true site. Or, if the intent is to disrupt rather than steal, hackers can alter orders—inflating them or changing prod-

ucts ordered—and then send them on to the true site for processing and delivery. Customers become dissatisfied with the improper order shipment, and the company may have huge inventory fluctuations that impact its operations.

In addition to threatening integrity, spoofing also threatens authenticity by making it difficult to discern the true sender of a message. Clever hackers can make it almost impossible to distinguish between a true and a fake identity or web address.

spam (junk) websites
also referred to as link farms; promise to offer products or services, but in fact are just collections of advertisements

Spam (junk) websites (also sometimes referred to as *link farms*) are a little different. These are sites that promise to offer some product or service, but in fact are just a collection of advertisements for other sites, some of which contain malicious code. For instance, you may search for "[name of town] weather," and then click on a link that promises your local weather, but then discover that all the site does is display ads for weather-related products or other websites. Junk or spam websites typically appear on search results, and do not involve e-mail. These sites cloak their identities by using domain names similar to legitimate firm names, and redirect traffic to known spammer-redirection domains such as topsearch10.com.

SNIFFING AND MAN-IN-THE-MIDDLE ATTACKS

sniffer
a type of eavesdropping program that monitors information traveling over a network

A **sniffer** is a type of eavesdropping program that monitors information traveling over a network. When used legitimately, sniffers can help identify potential network trouble-spots, but when used for criminal purposes, they can be damaging and very difficult to detect. Sniffers enable hackers to steal proprietary information from anywhere on a network, including passwords, e-mail messages, company files, and confidential reports. For instance, in 2013, five hackers were charged in another worldwide hacking scheme that targeted the corporate networks of retail chains such as 7-Eleven and the French retailer Carrefour SA, using sniffer programs to steal more than 160 million credit card numbers (Voreacos, 2013).

E-mail wiretaps are a variation on the sniffing threat. An e-mail wiretap is a method for recording or journaling e-mail traffic generally at the mail server level from any individual. E-mail wiretaps are used by employers to track employee messages, and by government agencies to surveil individuals or groups. E-mail wiretaps can be installed on servers and client computers. The USA PATRIOT Act permits the FBI to compel ISPs to install a black box on their mail servers that can impound the e-mail of a single person or group of persons for later analysis. In the case of American citizens communicating with other citizens, an FBI agent or government lawyer need only certify to a judge on the secret 11-member U.S. Foreign Intelligence Surveillance Court (FISC) that the information sought is relevant to an ongoing criminal investigation to get permission to install the program. Judges have no discretion. They must approve wiretaps based on government agents' unsubstantiated assertions. In the case of suspected terrorist activity, law enforcement does not have to inform a court prior to installing a wire or e-mail tap. A 2007 amendment to the 1978 Foreign Intelligence Surveillance Act, known as FISA, provided new powers to the National Security Agency to monitor international e-mail and telephone communications where one person is in the United States, and where the purpose of such interception is to collect foreign intelligence (Foreign Intelligence Surveillance Act of 1978; Protect America Act of 2007). The FISA Amendments Reauthorization Act of 2012 extends the provisions of FISA for five more

years, until 2017. NSA's XKeyscore program, revealed by Edward Snowden, is a form of "wiretap" that allows NSA analysts to search through vast databases containing not only e-mail, but online chats, and browsing histories of millions of individuals (Wills, 2013).

The Communications Assistance for Law Enforcement Act (CALEA) requires all communications carriers (including ISPs) to provide near-instant access to law enforcement agencies to their message traffic. Many Internet services (such as Facebook and LinkedIn) that have built-in ISP services technically are not covered by CALEA. One can only assume these non-ISP e-mail operators cooperate with law enforcement. Unlike the past where wiretaps required many hours to physically tap into phone lines, in today's digital phone systems, taps are arranged in a few minutes by the large carriers at their expense.

A **man-in-the-middle (MitM) attack** also involves eavesdropping but is more active than a sniffing attack, which typically involves passive monitoring. In a MitM attack, the attacker is able to intercept communications between two parties who believe they are directly communicating with one another, when in fact the attacker is controlling the communications. This allows the attacker to change the contents of the communication.

man-in-the-middle (MitM) attack
attack in which the attacker is able to intercept communications between two parties who believe they are directly communicating with one another, when in fact the attacker is controlling the communications

DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

In a **Denial of Service (DoS) attack**, hackers flood a website with useless pings or page requests that inundate and overwhelm the site's web servers. Increasingly, DoS attacks involve the use of bot networks and so-called "distributed attacks" built from thousands of compromised client computers. DoS attacks typically cause a website to shut down, making it impossible for users to access the site. For busy e-commerce sites, these attacks are costly; while the site is shut down, customers cannot make purchases. And the longer a site is shut down, the more damage is done to a site's reputation. Although such attacks do not destroy information or access restricted areas of the server, they can destroy a firm's online business. Often, DoS attacks are accompanied by attempts at blackmailing site owners to pay tens or hundreds of thousands of dollars to the hackers in return for stopping the DoS attack.

Denial of Service (DoS) attack
flooding a website with useless traffic to inundate and overwhelm the network

A **Distributed Denial of Service (DDoS) attack** uses hundreds or even thousands of computers to attack the target network from numerous launch points. DoS and DDoS attacks are threats to a system's operation because they can shut it down indefinitely. Major websites have experienced such attacks, making the companies aware of their vulnerability and the need to continually introduce new measures to prevent future attacks. According to Akamai, the number of DDoS attacks in the 2nd quarter of 2016 increased by about 130% compared to the same period in 2015. One new technique increasingly being used targets insecure routers and other home devices such as webcams that use UPnP (Universal Plug and Play) to amplify the attacks (Akamai, 2016a). With the growth of the Internet of Things (IoT), billions of Internet-connected things from refrigerators to security cameras can be used to launch service requests against servers. In October 2016, a large scale DDoS attack using Internet devices such as these was launched against an Internet domain resolving firm, Dyn. Twitter, Amazon, Netflix, Airbnb, the New York Times, and many other sites across the

Distributed Denial of Service (DDoS) attack
using numerous computers to attack the target network from numerous launch points

country were affected. Hackers were able to guess the administrator passwords of common devices (often set to factory defaults like admin, or 12345), and then insert instructions to launch an attack against Dyn servers (Sanger and Perlroth, 2016). DDoS attacks are typically isolated to a single firm, but in the Dyn attack, the firm attacked happened to be one of the switchboards for a large part of the Internet in the United States. In another measure of the prevalence of DDoS attacks, in an Arbor Networks survey of 354 ISP and network operators around the world, respondents noted that DDoS attacks against customers constituted the number one operational threat, with over 50% of respondents experiencing DDoS attacks during the survey period. Arbor Networks also reported that the size of reported DDoS attacks in terms of bandwidth consumed continued to increase in 2015, with attackers using reflection/amplification techniques to create attacks reaching 500 Gpbs (Arbor Networks, 2016). Another trend is DDoS smokescreening, in which attackers use DDoS as a distraction while they also insert malware or viruses or steal data. A 2016 survey of 760 security and IT professionals in companies in North America and Europe, the Middle East, and Africa conducted by Neustar found that 45% reported that a virus or malware was installed as a result of the DDoS attack, while 57% also experienced a theft of data or funds (Neustar, 2016). And not surprisingly, now that mobile data connections have become faster and more stable, hackers are beginning to harness mobile devices for mobile-based DDoS attacks. A recent attack originating from China used malicious ads loaded inside mobile apps and mobile browesrs as the attack mechanism (Majkowski, 2015).

China also appears to have been behind another major DDoS attack in 2015 against the software development platform GitHub, aimed specifically at two Chinese anti-censorship projects hosted on the platform. Researchers say the attack was an example of a new tool they have nicknamed the Great Cannon. Although originally thought to be part of China's Great Firewall censorship system, further investigation revealed that the Great Cannon is a separate distinct offensive system that is co-located with the Great Firewall. The Great Cannon enables hackers to hijack traffic to individual IP addresses and uses a man-in-the-middle attack to replace unencrypted content between a web server and the user with malicious Javascript that would load the two GitHub project pages every two seconds (Kirk, 2015b; Essers, 2015).

INSIDER ATTACKS

We tend to think of security threats to a business as originating outside the organization. In fact, the largest financial threats to business institutions come not from robberies but from embezzlement by insiders. Bank employees steal far more money than bank robbers. The same is true for e-commerce sites. Some of the largest disruptions to service, destruction to sites, and diversion of customer credit data and personal information have come from insiders—once trusted employees. Employees have access to privileged information, and, in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace. Research from Carnegie Mellon University documents the significant damage insiders have done to both private and public organizations (Software Engineering Institute, 2012). Survey results also indicate that insiders are more likely to be the source of cyberattacks than outsiders, and to cause more damage to an organization

than external attacks (PWC, 2015). In some instances, the insider might not have criminal intent, but inadvertently exposes data that can then be exploited by others. For instance, a Ponemon Institute study found that negligent insiders are a top cause of data breaches (Ponemon Institute, 2015b). Another study based on an analysis of the behavior of 10 million users during 2015 estimated that 1% of employees are responsible for 75% of cloud-related enterprise security risk, by reusing or sending out plain-text passwords, indiscriminately sharing fiiles, using risky applications, or accidentally downloading malware or clicking phishing links (Korolov, 2015).

POORLY DESIGNED SOFTWARE

Many security threats prey on poorly designed software, sometimes in the operating system and sometimes in the application software, including browsers. The increase in complexity and size of software programs, coupled with demands for timely delivery to markets, has contributed to an increase in software flaws or vulnerabilities that hackers can exploit. For instance, **SQL injection attacks** take advantage of vulnerabilities in poorly coded web application software that fails to properly validate or filter data entered by a user on a web page to introduce malicious program code into a company's systems and networks. An attacker can use this input validation error to send a rogue SQL query to the underlying database to access the database, plant malicious code, or access other systems on the network. Large web applications have hundreds of places for inputting user data, each of which creates an opportunity for an SQL injection attack. A large number of web-facing applications are believed to have SQL injection vulnerabilities, and tools are available for hackers to check web applications for these vulnerabilities.

SQL injection attack takes advantage of poorly coded web application software that fails to properly validate or filter data entered by a user on a web page

Each year, security firms identify thousands of software vulnerabilities in Internet browsers, PC, Macintosh, and Linux software, as well as mobile device operating systems and applications. According to Microsoft, vulnerability disclosures across the software industry in the second half of 2015 increased by 9% compared to the same period in 2014. Over 3,300 vulnerabilities were identified (Microsoft, 2016). Browser vulnerabilities in particular are a popular target, as well as browser plug-ins such as for Adobe Reader. A **zero-day vulnerability** is one that has been previously unreported and for which no patch yet exists. In 2015, 54 zero-day vulnerabilities were reported, up from 24 in 2014 (Symantec, 2016). The very design of the personal computer includes many open communication ports that can be used, and indeed are designed to be used, by external computers to send and receive messages. Ports that are frequently attacked include TCP port 445 (Microsoft-DS), port 80 (WWW/HTTP), and 443 (SSL/HTTPS). Given their complexity and design objectives, all operating systems and application software, including Linux and Macintosh, have vulnerabilities.

zero-day vulnerability software vulnerability that has been previously unreported and for which no patch yet exists

In 2014, a flaw in the OpenSSL encryption system, used by millions of websites, known as the **Heartbleed bug**, was discovered (see Section 5.3 for a further discussion of SSL). The vulnerability allowed hackers to decrypt an SSL session and discover user names, passwords, and other user data, by using OpenSSL in combination with a communications protocol called the RFC6520 heartbeat that helps a remote user remain in touch after connecting with a website server. In the process a small chunk of the server's memory content can leak out (hence the name heartbleed), potentially large

Heartbleed bug flaw in OpenSSL encryption system that allowed hackers to decrypt an SSL session and discover user names, passwords, and other user data

enough to hold a password or encryption key that would allow a hacker to exploit the server further. The Heartbleed bug also affected over 1,300 Android apps. Later in 2014, another vulnerability known as ShellShock or BashBug that affected most versions of Linux and Unix, as well as Mac OS X, was revealed. ShellShock enabled attackers to use CGI (see Chapter 4) to add malicious commands (Symantec, 2015). In 2015, researchers announced that they had discovered a new SSL/TLS vulnerability that they named FREAK (Factoring Attack on RSA-Export Keys) that allows man-in-the-middle attacks that enable the interception and decryption of encrypted communications between clients and servers, which would then allow the attackers to steal passwords and other personal information. More than 60% of encrypted websites were reportedly open to attack via this security vulnerability, including those for the White House, the FBI, and the National Security Agency (Hackett, 2015; Vaughan-Nichols, 2015). A recent study found over 1,200 of the largest firms' websites have not fixed the problem entirely.

SOCIAL NETWORK SECURITY ISSUES

Social networks like Facebook, Twitter, LinkedIn, Pinterest, and Tumblr provide a rich and rewarding environment for hackers. Viruses, site takeovers, identity fraud, malware-loaded apps, click hijacking, phishing, and spam are all found on social networks. According to Symantec, the most common type of scam on social media sites in 2015 were manual sharing scams, where victims unwittingly shared videos, stories, and pictures that included links to malicious sites. Fake offerings that invite victims to join a fake event or group with incentives such as free gift cards and that require a user to share his or her information with the attacker were another common technique. Other techniques include fake Like buttons that, when clicked, install malware and post updates to the user's Newsfeed, further spreading the attack, and fake apps (Symantec, 2016). By sneaking in among our friends, hackers can masquerade as friends and dupe users into scams.

Social network firms have thus far been relatively poor policemen because they have failed to aggressively weed out accounts that send visitors to malware sites (unlike Google, which maintains a list of known malware sites and patrols its search results looking for links to malware sites). Social networks are open: anyone can set up a personal page, even criminals. Most attacks are social engineering attacks that tempt visitors to click on links that sound reasonable. Social apps downloaded from either the social network or a foreign site are not certified by the social network to be clean of malware. It's "clicker beware."

MOBILE PLATFORM SECURITY ISSUES

The explosion in mobile devices has broadened opportunities for hackers. Mobile users are filling their devices with personal and financial information, and using them to conduct an increasing number of transactions, from retail purchases to mobile banking, making them excellent targets for hackers. In general, mobile devices face all the same risks as any Internet device as well as some new risks associated with wireless network security. For instance, public Wi-Fi networks that are not secured are very susceptible to hacking. While most PC users are aware their computers and websites may be hacked and contain malware, most cell phone users believe their cell

phone is as secure as a traditional landline phone. As with social network members, mobile users are prone to think they are in a shared, trustworthy environment.

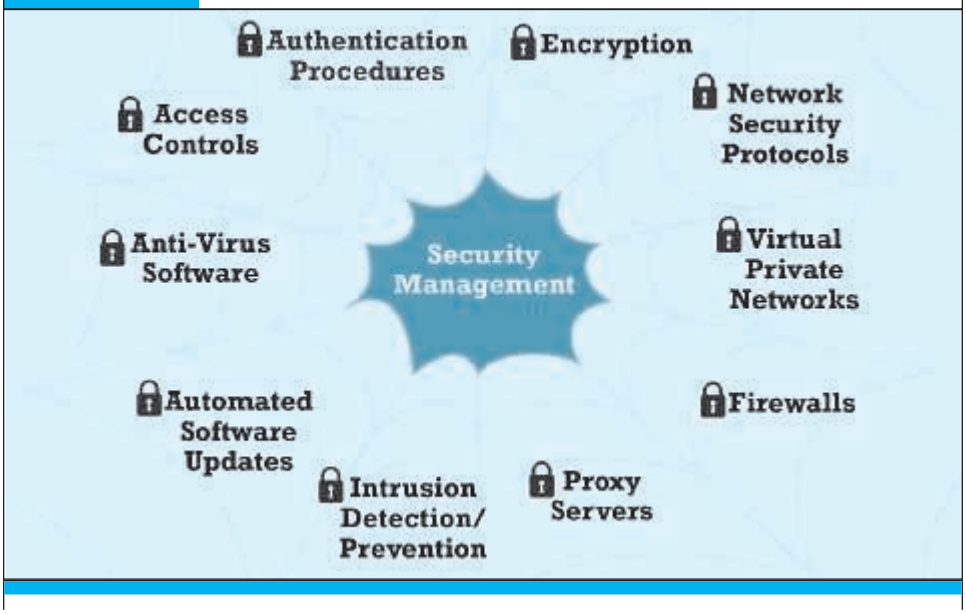
Mobile cell phone malware (sometimes referred to as malicious mobile apps (MMAs) or rogue mobile apps) was developed as early as 2004 with Cabir, a Bluetooth worm affecting Symbian operating systems (Nokia phones) and causing the phone to continuously seek out other Bluetooth-enabled devices, quickly draining the battery. The iKee.B worm, first discovered in 2009, only two years after the iPhone was introduced, infected jailbroken iPhones, turning the phones into botnet-controlled devices. An iPhone in Europe could be hacked by an iPhone in the United States, and all its private data sent to a server in Poland. IKee.B established the feasibility of cell phone botnets.

In 2015, Symantec analyzed 10 million apps and found 3 million were malware. Symantec expects the growth in mobile malware to continue in 2016 and become more aggressive in targeting mobile payment and mobile banking applications. The majority of mobile malware still targets the Android platform. For instance, Symantec has already discovered Android malware that can intercept text messages with bank authentication codes and forward them to attackers, as well as fake versions of legitimate mobile banking applications. However, the Apple iPhone platform is beginning to be increasingly targeted as well, and in 2015, Chinese hackers infected Xcode, Apple's integrated suite of development tools for creating iOS appps, and as a result, unsuspecting Chinese iOS developers unknowingly created thousands of apps with the malicious code (Keizer, 2015). And it is not just rogue applications that are dangerous, but also popular legitimate applications that simply have little protection from hackers. For instance, in 2014, security researchers revealed that the Starbucks mobile app, the most used mobile payment app in the United States, was storing user names, e-mail addresses, and passwords in clear text, in such a way that anyone with access to the phone could see the passwords and user names by connecting the phone to a computer. According to researchers, Starbucks erred in emphasizing convenience and ease of use in the design of the app over security concerns (Schuman, 2014).

Vishing attacks target gullible cell phone users with verbal messages to call a certain number and, for example, donate money to starving children in Haiti. *Smishing* attacks exploit SMS/text messages. Compromised text messages can contain e-mail and website addresses that can lead the innocent user to a malware site. Criminal SMS spoofing services have emerged, which conceal the cybercriminal's true phone number, replacing it with a false alpha-numeric name. SMS spoofing can also be used by cybercriminals to lure mobile users to a malicious website by sending a text that appears to be from a legitimate organization in the From field, and suggesting the receiver click on a malicious URL hyperlink to update an account or obtain a gift card. A small number of downloaded apps from app stores have also contained malware. *Madware*—innocent-looking apps that contain adware that launches pop-up ads and text messages on your mobile device—is also becoming an increasing problem. An examination of 3 million apps in 2015 that Symantec classified as grayware (programs that do not contain viruses and are not overtly malicious, but which can be annoying or harmful) found that 2.3 million of those ads were madware (Symantec, 2016).

Read the *Insight on Technology* case, *Think Your Smartphone Is Secure?* for a further discussion of some of the issues surrounding smartphone security.

FIGURE 5.5 TOOLS AVAILABLE TO ACHIEVE SITE SECURITY



There are a number of tools available to achieve site security.

5.3 TECHNOLOGY SOLUTIONS

At first glance, it might seem like there is not much that can be done about the onslaught of security breaches on the Internet. Reviewing the security threats in the previous section, it is clear that the threats to e-commerce are very real, widespread, global, potentially devastating for individuals, businesses, and entire nations, and likely to be increasing in intensity along with the growth in e-commerce and the continued expansion of the Internet. But in fact a great deal of progress has been made by private security firms, corporate and home users, network administrators, technology firms, and government agencies. There are two lines of defense: technology solutions and policy solutions. In this section, we consider some technology solutions, and in the following section, we look at some policy solutions that work.

The first line of defense against the wide variety of security threats to an e-commerce site is a set of tools that can make it difficult for outsiders to invade or destroy a site. **Figure 5.5** illustrates the major tools available to achieve site security.

PROTECTING INTERNET COMMUNICATIONS

Because e-commerce transactions must flow over the public Internet, and therefore involve thousands of routers and servers through which the transaction packets flow, security experts believe the greatest security threats occur at the level of Internet communications. This is very different from a private network where a dedicated communication line is established between two parties. A number of tools are available to protect the security of Internet communications, the most basic of which is message encryption.

ENCRYPTION

Encryption is the process of transforming plain text or data into **cipher text** that cannot be read by anyone other than the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission. Encryption can provide four of the six key dimensions of e-commerce security referred to in Table 5.3 on page 260:

- *Message integrity*—provides assurance that the message has not been altered.
- *Nonrepudiation*—prevents the user from denying he or she sent the message.
- *Authentication*—provides verification of the identity of the person (or computer) sending the message.
- *Confidentiality*—gives assurance that the message was not read by others.

This transformation of plain text to cipher text is accomplished by using a key or cipher. A **key** (or **cipher**) is any method for transforming plain text to cipher text.

Encryption has been practiced since the earliest forms of writing and commercial transactions. Ancient Egyptian and Phoenician commercial records were encrypted using substitution and transposition ciphers. In a **substitution cipher**, every occurrence of a given letter is replaced systematically by another letter. For instance, if we used the cipher "letter plus two"—meaning replace every letter in a word with a new letter two places forward—then the word "Hello" in plain text would be transformed into the following cipher text: "JGNNQ." In a **transposition cipher**, the ordering of the letters in each word is changed in some systematic way. Leonardo Da Vinci recorded his shop notes in reverse order, making them readable only with a mirror. The word "Hello" can be written backwards as "OLLEH." A more complicated cipher would (a) break all words into two words and (b) spell the first word with every other letter beginning with the first letter, and then spell the second word with all the remaining letters. In this cipher, "HELLO" would be written as "HLO EL."

encryption
the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission

cipher text
text that has been encrypted and thus cannot be read by anyone other than the sender and the receiver

key (cipher)
any method for transforming plain text to cipher text

substitution cipher
every occurrence of a given letter is replaced systematically by another letter

transposition cipher
the ordering of the letters in each word is changed in some systematic way

Symmetric Key Cryptography

In order to decipher (decrypt) these messages, the receiver would have to know the secret cipher that was used to encrypt the plain text. This is called **symmetric key cryptography** or **secret key cryptography**. In symmetric key cryptography, both the sender and the receiver use the same key to encrypt and decrypt the message. How do the sender and the receiver have the same key? They have to send it over some communication media or exchange the key in person. Symmetric key cryptography was used extensively throughout World War II and is still a part of Internet cryptography.

The possibilities for simple substitution and transposition ciphers are endless, but they all suffer from common flaws. First, in the digital age, computers are so powerful and fast that these ancient means of encryption can be broken quickly. Second, symmetric key cryptography requires that both parties share the same key. In order to share the same key, they must send the key over a presumably *insecure* medium where it could be stolen and used to decipher messages. If the secret key is lost or stolen, the entire encryption system fails. Third, in commercial use, where we are not all part of the same team, you would need a secret key for each of the parties with whom you transacted, that is, one key for the bank, another for the department store,

symmetric key cryptography (secret key cryptography)
both the sender and the receiver use the same key to encrypt and decrypt the message

and another for the government. In a large population of users, this could result in as many as $n^{(n-1)}$ keys. In a population of millions of Internet users, thousands of millions of keys would be needed to accommodate all e-commerce customers (estimated at about 177 million in the United States). Potentially, 177^2 million different keys would be needed. Clearly this situation would be too unwieldy to work in practice.

Modern encryption systems are digital. The ciphers or keys used to transform plain text into cipher text are digital strings. Computers store text or other data as binary strings composed of 0s and 1s. For instance, the binary representation of the capital letter "A" in ASCII computer code is accomplished with eight binary digits (bits): 01000001. One way in which digital strings can be transformed into cipher text is by multiplying each letter by another binary number, say, an eight-bit key number 0101 0101. If we multiplied every digital character in our text messages by this eight-bit key and sent the encrypted message to a friend along with the secret eight-bit key, the friend could decode the message easily.

The strength of modern security protection is measured in terms of the length of the binary key used to encrypt the data. In the preceding example, the eight-bit key is easily deciphered because there are only 2^8 or 256 possibilities. If the intruder knows you are using an eight-bit key, then he or she could decode the message in a few seconds using a modern desktop PC just by using the brute force method of checking each of the 256 possible keys. For this reason, modern digital encryption systems use keys with 56, 128, 256, or 512 binary digits. With encryption keys of 512 digits, there are 2^{512} possibilities to check out. It is estimated that all the computers in the world would need to work for 10 years before stumbling upon the answer.

Data Encryption Standard (DES) developed by the National Security Agency (NSA) and IBM. Uses a 56-bit encryption key

Advanced Encryption Standard (AES) the most widely used symmetric key algorithm, offering 128-, 192-, and 256-bit keys

The **Data Encryption Standard (DES)** was developed by the National Security Agency (NSA) and IBM in the 1950s. DES uses a 56-bit encryption key. To cope with much faster computers, it has been improved by the *Triple DES Encryption Algorithm (TDEA)*—essentially encrypting the message three times, each with a separate key. Today, the most widely used symmetric key algorithm is **Advanced Encryption Standard (AES)**, which offers key sizes of 128, 192, and 256 bits. AES had been considered to be relatively secure, but in 2011, researchers from Microsoft and a Belgian university announced that they had discovered a way to break the algorithm, and with this work, the "safety margin" of AES continues to erode. There are also many other symmetric key systems that are currently less widely used, with keys up to 2,048 bits.[1]

Public Key Cryptography

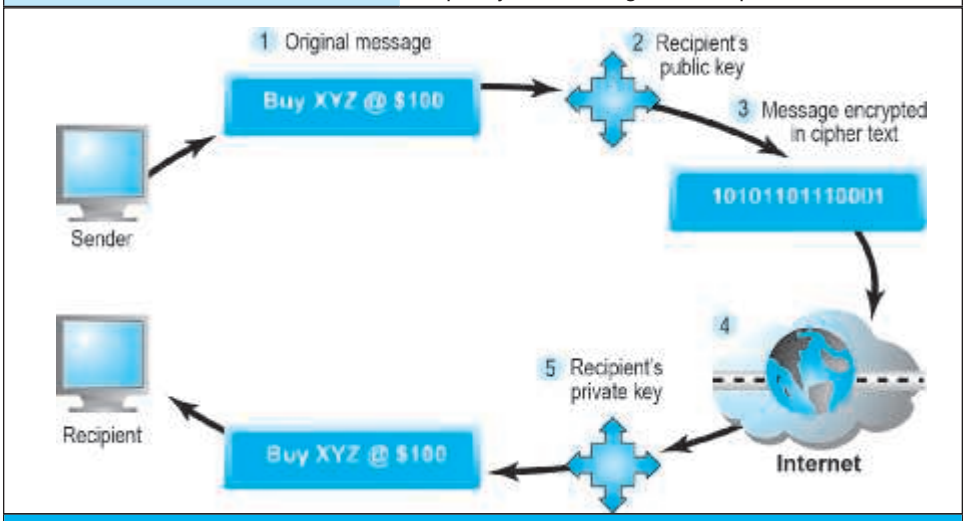
public key cryptography two mathematically related digital keys are used: a public key and a private key. The private key is kept secret by the owner, and the public key is widely disseminated. Both keys can be used to encrypt and decrypt a message. However, once the keys are used to encrypt a message, that same key cannot be used to unencrypt the message

In 1976, a new way of encrypting messages called **public key cryptography** was invented by Whitfield Diffie and Martin Hellman. Public key cryptography (also referred to as *asymmetric cryptography*) solves the problem of exchanging keys. In this method, two mathematically related digital keys are used: a public key and a private key. The private key is kept secret by the owner, and the public key is widely disseminated. Both keys can be used to encrypt and decrypt a message. However, once the keys are used

[1] For instance: DESX, GDES, and RDES with 168-bit keys; the RC Series: RC2, RC4, and RC5 with keys up to 2,048 bits; and the IDEA algorithm, the basis of PGP, e-mail public key encryption software described later in this chapter, which uses 128-bit keys.

FIGURE 5.6 PUBLIC KEY CRYPTOGRAPHY—A SIMPLE CASE

STEP	DESCRIPTION
1. The sender creates a digital message.	The message could be a document, spreadsheet, or any digital object.
2. The sender obtains the recipient's public key from a public directory and applies it to the message.	Public keys are distributed widely and can be obtained from recipients directly.
3. Application of the recipient's key produces an encrypted cipher text message.	Once encrypted using the public key, the message cannot be reverse-engineered or unencrypted using the same public key. The process is irreversible.
4. The encrypted message is sent over the Internet.	The encrypted message is broken into packets and sent through several different pathways, making interception of the entire message difficult (but not impossible).
5. The recipient uses his/her private key to decrypt the message.	The only person who can decrypt the message is the person who has possession of the recipient's private key. Hopefully, this is the legitimate recipient.



In the simplest use of public key cryptography, the sender encrypts a message using the recipient's public key, and then sends it over the Internet. The only person who can decrypt this message is the recipient, using his or her private key. However, this simple case does not ensure integrity or an authentic message.

to encrypt a message, the same key cannot be used to unencrypt the message. The mathematical algorithms used to produce the keys are one-way functions. A *one-way irreversible mathematical function* is one in which, once the algorithm is applied, the input cannot be subsequently derived from the output. Most food recipes are like this. For instance, it is easy to make scrambled eggs, but impossible to retrieve whole eggs from the scrambled eggs. Public key cryptography is based on the idea of irreversible mathematical functions. The keys are sufficiently long (128, 256, and 512 bits) that it would take enormous computing power to derive one key from the other using the largest and fastest computers available. **Figure 5.6** illustrates a simple use of public key cryptography and takes you through the important steps in using public and private keys.

Public Key Cryptography Using Digital Signatures and Hash Digests

In public key cryptography, some elements of security are missing. Although we can be quite sure the message was not understood or read by a third party (message confidentiality), there is no guarantee the sender really is the sender; that is, there is no authentication of the sender. This means the sender could deny ever sending the message (repudiation). And there is no assurance the message was not altered somehow in transit. For example, the message "Buy Cisco @ $16" could have been accidentally or intentionally altered to read "Sell Cisco @ $16." This suggests a potential lack of integrity in the system.

A more sophisticated use of public key cryptography can achieve authentication, nonrepudiation, and integrity. **Figure 5.7** illustrates this more powerful approach.

hash function
an algorithm that produces a fixed-length number called a hash or message digest

To check the integrity of a message and ensure it has not been altered in transit, a hash function is used first to create a digest of the message. A **hash function** is an algorithm that produces a fixed-length number called a *hash* or *message digest.* A hash function can be simple, and count the number of digital 1s in a message, or it can be more complex, and produce a 128-bit number that reflects the number of 0s and 1s, the number of 00s and 11s, and so on. Standard hash functions are available (MD4 and MD5 produce 128- and 160-bit hashes) (Stein, 1998). These more complex hash functions produce hashes or hash results that are unique to every message. The results of applying the hash function are sent by the sender to the recipient. Upon receipt, the recipient applies the hash function to the received message and checks to verify the same result is produced. If so, the message has not been altered. The sender then encrypts both the hash result and the original message using the recipient's public key (as in Figure 5.6 on page 289), producing a single block of cipher text.

digital signature (e-signature)
"signed" cipher text that can be sent over the Internet

One more step is required. To ensure the authenticity of the message and to ensure nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender's private key. This produces a **digital signature** (also called an *e-signature*) or "signed" cipher text that can be sent over the Internet.

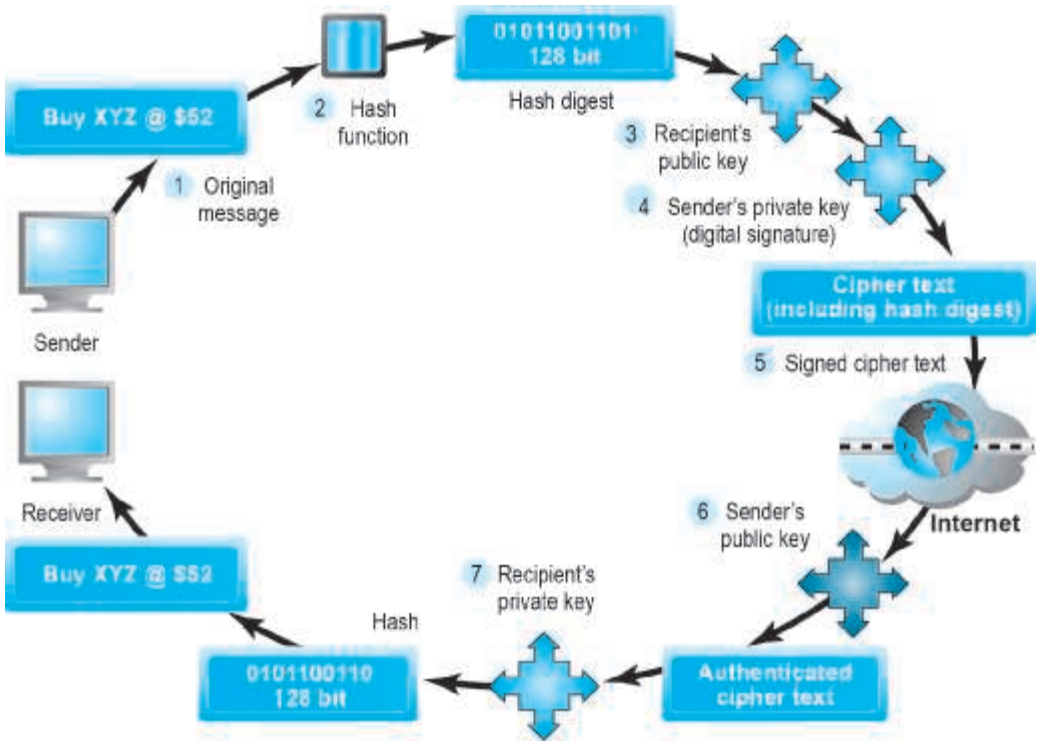
A digital signature is a close parallel to a handwritten signature. Like a handwritten signature, a digital signature is unique—only one person presumably possesses the private key. When used with a hash function, the digital signature is even more unique than a handwritten signature. In addition to being exclusive to a particular individual, when used to sign a hashed document, the digital signature is also unique to the document, and changes for every document.

The recipient of this signed cipher text first uses the sender's public key to authenticate the message. Once authenticated, the recipient uses his or her private key to obtain the hash result and original message. As a final step, the recipient applies the same hash function to the original text, and compares the result with the result sent by the sender. If the results are the same, the recipient now knows the message has not been changed during transmission. The message has integrity.

Early digital signature programs required the user to have a digital certificate, and were far too difficult for an individual to use. Newer programs are Internet-based and do not require users to install software, or understand digital certificate technology. DocuSign, Adobe eSign, and Sertifi are among a number of companies offering online

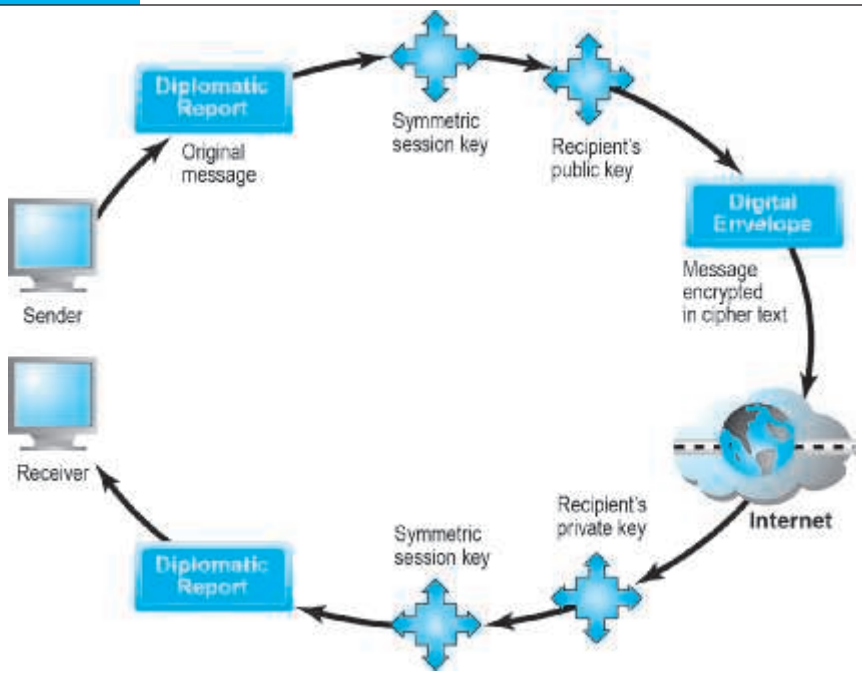
FIGURE 5.7 PUBLIC KEY CRYPTOGRAPHY WITH DIGITAL SIGNATURES

STEP	DESCRIPTION
1. The sender creates an original message.	The message can be any digital file.
2. The sender applies a hash function, producing a 128-bit hash result.	Hash functions create a unique digest of the message based on the message contents.
3. The sender encrypts the message and hash result using the recipient's public key.	This irreversible process creates a cipher text that can be read only by the recipient using his or her private key.
4. The sender encrypts the result, again using his or her private key.	The sender's private key is a digital signature. There is only one person who can create this digital mark.
5. The result of this double encryption is sent over the Internet.	The message traverses the Internet as a series of independent packets.
6. The receiver uses the sender's public key to authenticate the message.	Only one person can send this message, namely, the sender.
7. The receiver uses his or her private key to decrypt the hash function and the original message. The receiver checks to ensure the original message and the hash function results conform to one another.	The hash function is used here to check the original message. This ensures the message was not changed in transit.



A more realistic use of public key cryptography uses hash functions and digital signatures to both ensure the confidentiality of the message and authenticate the sender. The only person who could have sent the above message is the owner or the sender using his/her private key. This authenticates the message. The hash function ensures the message was not altered in transit. As before, the only person who can decipher the message is the recipient, using his/her private key.

FIGURE 5.8 PUBLIC KEY CRYPTOGRAPHY: CREATING A DIGITAL ENVELOPE



A digital envelope can be created to transmit a symmetric key that will permit the recipient to decrypt the message and be assured the message was not intercepted in transit.

digital signature solutions. Many insurance, finance, and surety companies now permit customers to electronically sign documents.

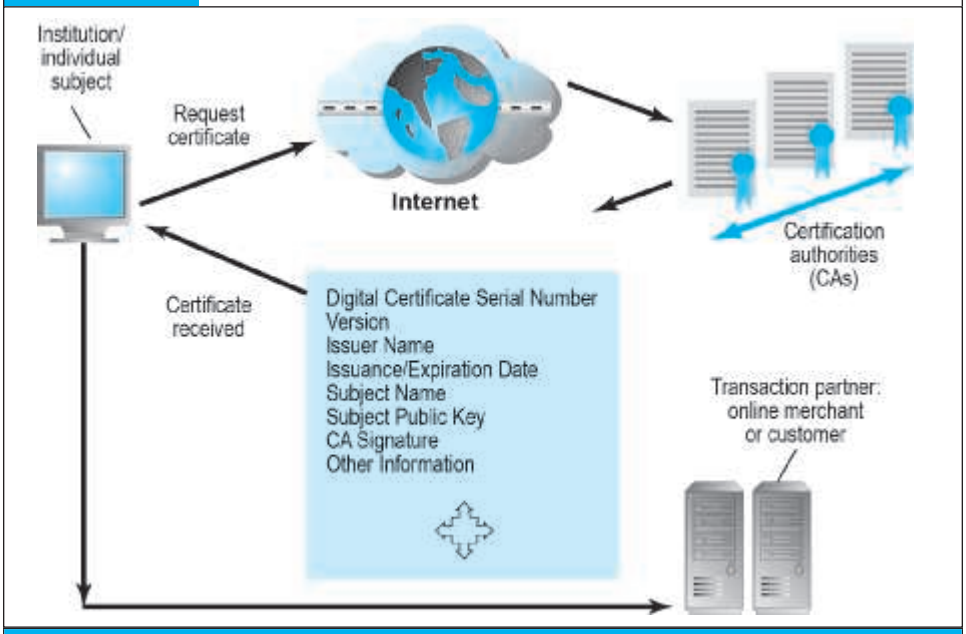
Digital Envelopes

Public key cryptography is computationally slow. If one used 128- or 256-bit keys to encode large documents—such as this chapter or the entire book—significant declines in transmission speeds and increases in processing time would occur. Symmetric key cryptography is computationally faster, but as we pointed out previously, it has a weakness—namely, the symmetric key must be sent to the recipient over insecure transmission lines. One solution is to use the more efficient symmetric encryption and decryption for large documents, but public key cryptography to encrypt and send the symmetric key. This technique is called using a **digital envelope**. See **Figure 5.8** for an illustration of how a digital envelope works.

digital envelope
a technique that uses symmetric encryption for large documents, but public key cryptography to encrypt and send the symmetric key

In Figure 5.8, a diplomatic document is encrypted using a symmetric key. The symmetric key—which the recipient will require to decrypt the document—is itself encrypted, using the recipient's public key. So we have a "key within a key" (a *digital envelope*). The encrypted report and the digital envelope are sent across the Web. The recipient first uses his/her private key to decrypt the symmetric key, and then

FIGURE 5.9 DIGITAL CERTIFICATES AND CERTIFICATION AUTHORITIES



The PKI includes certification authorities that issue, verify, and guarantee digital certificates that are used in e-commerce to assure the identity of transaction partners.

the recipient uses the symmetric key to decrypt the report. This method saves time because both encryption and decryption are faster with symmetric keys.

Digital Certificates and Public Key Infrastructure (PKI)

There are still some deficiencies in the message security regime described previously. How do we know that people and institutions are who they claim to be? Anyone can make up a private and public key combination and claim to be someone they are not. Before you place an order with an online merchant such as Amazon, you want to be sure it really is Amazon you have on the screen and not a spoofer masquerading as Amazon. In the physical world, if someone asks who you are and you show a social security number, they may well ask to see a picture ID or a second form of certifiable or acceptable identification. If they really doubt who you are, they may ask for references to other authorities and actually interview these other authorities. Similarly, in the digital world, we need a way to know who people and institutions really are.

Digital certificates, and the supporting public key infrastructure, are an attempt to solve this problem of digital identity. A **digital certificate** is a digital document issued by a trusted third-party institution known as a **certification authority (CA)** that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority (the name of the CA encrypted using the CA's private key), and other identifying information (see **Figure 5.9**).

digital certificate
a digital document issued by a certification authority that contains a variety of identifying information

certification authority (CA)
a trusted third party that issues digital certificates

public key infrastructure (PKI)
CAs and digital certificate procedures that are accepted by all parties

In the United States, private corporations such as VeriSign, browser manufacturers, security firms, and government agencies such as the U.S. Postal Service and the Federal Reserve issue CAs. Worldwide, thousands of organizations issue CAs. A hierarchy of CAs has emerged with less-well-known CAs being certified by larger and better-known CAs, creating a community of mutually verifying institutions. **Public key infrastructure (PKI)** refers to the CAs and digital certificate procedures that are accepted by all parties. When you sign into a "secure" site, the URL will begin with "https" and a closed lock icon will appear on your browser. This means the site has a digital certificate issued by a trusted CA. It is not, presumably, a spoof site.

To create a digital certificate, the user generates a public/private key pair and sends a request for certification to a CA along with the user's public key. The CA verifies the information (how this is accomplished differs from CA to CA). The CA issues a certificate containing the user's public key and other related information. Finally, the CA creates a message digest from the certificate itself (just like a hash digest) and signs it with the CA's private key. This signed digest is called the *signed certificate*. We end up with a totally unique cipher text document—there can be only one signed certificate like this in the world.

There are several ways the certificates are used in commerce. Before initiating a transaction, the customer can request the signed digital certificate of the merchant and decrypt it using the merchant's public key to obtain both the message digest and the certificate as issued. If the message digest matches the certificate, then the merchant and the public key are authenticated. The merchant may in return request certification of the user, in which case the user would send the merchant his or her individual certificate. There are many types of certificates: personal, institutional, web server, software publisher, and CAs themselves.

PKI and CAs can also be used to secure software code and content for applications that are directly downloaded to mobile devices from the Internet. Using a technique referred to as code signing, mobile application developers use their private key to encrypt a digital signature. When end users decrypt the signature with the corresponding public key, it confirms the developer's identity and the integrity of the code.

Pretty Good Privacy (PGP)
a widely used e-mail public key encryption software program

You can easily obtain a public and private key for personal, noncommercial use at the International PGP Home Page website, Pgpi.org. **Pretty Good Privacy (PGP)** was invented in 1991 by Phil Zimmerman, and has become one of the most widely used e-mail public key encryption software tools in the world. Using PGP software installed on your computer, you can compress and encrypt your messages as well as authenticate both yourself and the recipient. There are also a number of Firefox, Chrome, Internet Explorer, and Safari add-ons, extensions, or plug-ins that enable you to encrypt your e-mail.

Limitations of PKI

PKI is a powerful technological solution to security issues, but it has many limitations, especially concerning CAs. PKI applies mainly to protecting messages in transit on the Internet and is not effective against insiders—employees—who have legitimate access to corporate systems including customer information. Most e-commerce sites

Unit 3 & 4

TABLE 5.7 GOVERNMENT EFFORTS TO REGULATE AND CONTROL ENCRYPTION

REGULATORY EFFORT	IMPACT
Restricted export of strong security systems	Supported primarily by the United States. Widespread distribution of encryption schemes weakens this policy. The policy is changing to permit exports except to pariah countries.
Key escrow/key recovery schemes	France, the United Kingdom, and the United States supported this effort in the late 1990s but now have largely abandoned it. There are few trusted third parties.
Lawful access and forced disclosure	Growing support in U.S. legislation and in OECD countries.
Official hacking	All countries are rapidly expanding budgets and training for law enforcement "technical centers" aimed at monitoring and cracking computer-based encryption activities of suspected criminals.

5.5 E-COMMERCE PAYMENT SYSTEMS

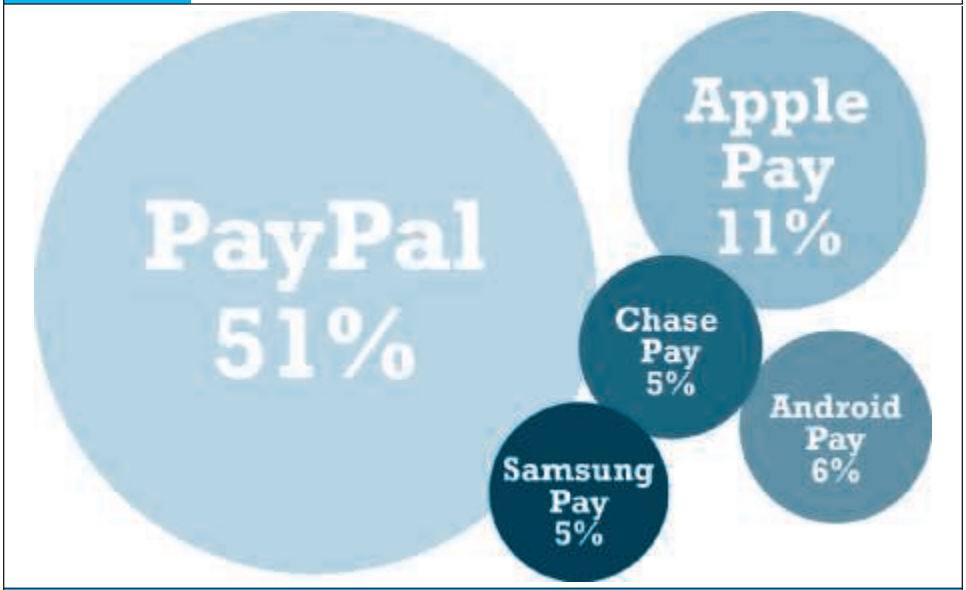
For the most part, existing payment mechanisms such as cash, credit cards, debit cards, checking accounts, and stored value accounts have been able to be adapted to the online environment, albeit with some significant limitations that have led to efforts to develop alternatives. In addition, new types of purchasing relationships, such as between individuals online, and new technologies, such as the development of the mobile platform, have also created both a need and an opportunity for the development of new payment systems. In this section, we provide an overview of the major e-commerce payment systems in use today. **Table 5.8** lists some of the major trends in e-commerce payments in 2016–2017.

U.S. online payments represent a market of almost $600 billion in 2016, and are expected to grow an additional $332 billion to around $932 billion by 2020. Institutions and business firms that can handle this volume of transactions (mostly the large

TABLE 5.8 MAJOR TRENDS IN E-COMMERCE PAYMENTS 2016–2017

- Payment by credit and/or debit card remains the dominant form of online payment.
- Mobile retail payment volume skyrockets.
- PayPal remains the most popular alternative payment method online.
- Apple, Google, Samsung, and PayPal extend their reach in mobile payment apps.
- Large banks enter the mobile wallet and P2P payments market.
- Square gains further traction with a smartphone app, credit card reader, and credit card processing service that permits anyone to accept credit card payments.
- Google refocuses Google Wallet, which had met with tepid response, solely on sending and receiving money.
- Mobile P2P payment systems such as Venmo take off.

FIGURE 5.13 ALTERNATIVE PAYMENT METHODS USED BY U.S. CONSUMERS



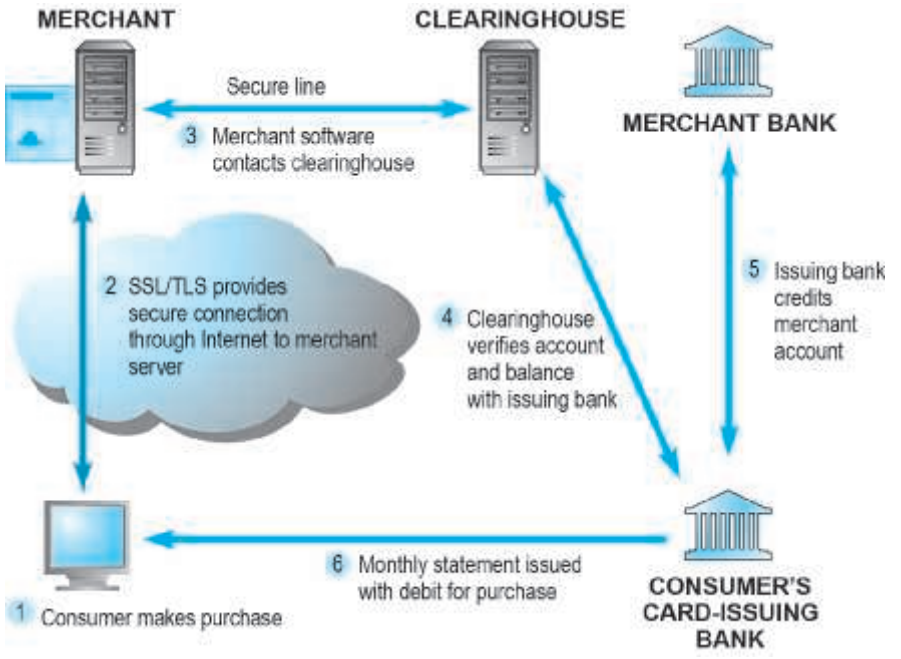
PayPal is still, by far, the most popular alternative payment method.
SOURCE: Based on data from eMarketer, 2016a.

banking and credit firms) generally extract 2%–3% of the transactions in the form of fees, or about $18 billion a year in revenue. Given the size of the market, competition for online payments is spirited. New forms of online payment are expected to attract a substantial part of this growth.

In the United States, the primary form of online payment is still the existing credit and debit card system. Alternative payment methods such as PayPal continue to make inroads into traditional payment methods. Mobile payments are also expected to grow significantly. **Figure 5.13** illustrates the percentage of consumers that use various alternative payment methods in 2016. However, none of these alternative payment methods have become substitutes for the bank and credit cards, but instead provide consumers with alternative methods of accessing their existing bank and credit accounts.

In other parts of the world, e-commerce payments can be very different depending on traditions and infrastructure. Credit cards are not nearly as dominant a form of online payment as they are in the United States. If you plan on operating an e-commerce site in Europe, Asia, or Latin America, you will need to develop different payment systems for each region. For instance, in Denmark, Norway, and Finland payment is primarily with debit or credit cards, while in Sweden, payment after being tendered an invoice and by bank transfer are very popular in addition to credit/debit cards. In the Netherlands, the online payments service iDEAL is the most popular retail e-commerce payment method. In Italy, consumers rely heavily on both credit

FIGURE 5.14 HOW AN ONLINE CREDIT CARD TRANSACTION WORKS



cards and PayPal. In Japan, although credit card is the primary payment method, many consumers still pick up and pay for goods using cash at local convenience stores (konbini) (eMarketer, Inc., 2015).

ONLINE CREDIT CARD TRANSACTIONS

Because credit and debit cards are the dominant form of online payment, it is important to understand how they work and to recognize the strengths and weaknesses of this payment system. Online credit card transactions are processed in much the same way that in-store purchases are, with the major differences being that online merchants never see the actual card being used, no card impression is taken, and no signature is available. Online credit card transactions most closely resemble Mail Order-Telephone Order (MOTO) transactions. These types of purchases are also called Cardholder Not Present (CNP) transactions and are the major reason that charges can be disputed later by consumers. Because the merchant never sees the credit card, nor receives a hand-signed agreement to pay from the customer, when disputes arise, the merchant faces the risk that the transaction may be disallowed and reversed, even though he has already shipped the goods or the user has downloaded a digital product.

Figure 5.14 illustrates the online credit card purchasing cycle. There are five parties involved in an online credit card purchase: consumer, merchant, clearinghouse, merchant bank (sometimes called the "acquiring bank"), and the consumer's card-issuing bank. In order to accept payments by credit card, online merchants must have

merchant account
a bank account that allows companies to process credit card payments and receive funds from those transactions

a merchant account established with a bank or financial institution. A **merchant account** is simply a bank account that allows companies to process credit card payments and receive funds from those transactions.

As shown in Figure 5.14, an online credit card transaction begins with a purchase (1). When a consumer wants to make a purchase, he or she adds the item to the merchant's shopping cart. When the consumer wants to pay for the items in the shopping cart, a secure tunnel through the Internet is created using SSL/TLS. Using encryption, SSL/TLS secures the session during which credit card information will be sent to the merchant and protects the information from interlopers on the Internet (2). SSL does not authenticate either the merchant or the consumer. The transacting parties have to trust one another.

Once the consumer credit card information is received by the merchant, the merchant software contacts a clearinghouse (3). As previously noted, a clearinghouse is a financial intermediary that authenticates credit cards and verifies account balances. The clearinghouse contacts the issuing bank to verify the account information (4). Once verified, the issuing bank credits the account of the merchant at the merchant's bank (usually this occurs at night in a batch process) (5). The debit to the consumer account is transmitted to the consumer in a monthly statement (6).

Credit Card E-commerce Enablers

Companies that have a merchant account still need to buy or build a means of handling the online transaction; securing the merchant account is only step one in a two-part process. Today, Internet payment service providers (sometimes referred to as payment gateways) can provide both a merchant account and the software tools needed to process credit card purchases online.

For instance, Authorize.net is an Internet payment service provider. The company helps a merchant secure an account with one of its merchant account provider partners and then provides payment processing software for installation on the merchant's server. The software collects the transaction information from the merchant's site and then routes it via the Authorize.net "payment gateway" to the appropriate bank, ensuring that customers are authorized to make their purchases. The funds for the transaction are then transferred to the merchant's merchant account. CyberSource is another well-known Internet payment service provider.

PCI-DSS Compliance

PCI-DSS (Payment Card Industry-Data Security Standards)
data security standards instituted by the five major credit card companies

The **PCI-DSS (Payment Card Industry-Data Security Standard)** is a data security standard instituted by the five major credit card companies (Visa, MasterCard, American Express, Discover, and JCB). PCI-DSS is not a law or governmental regulation, but an industry-mandated standard. Every online merchant must comply with the appropriate level of PCI-DSS in order to accept credit card payments. Those that fail to comply and are involved in a credit card breach may ultimately be subjected to fines and other expenses. PCI-DSS has various levels, related to the number of credit and/or debit cards processed by the merchant each year. Level 1, the strictest level, applies to very large merchants that process more than 6 million transactions a year, while Level 2 applies to those who process between 1 million and 6 million. Level 3

applies to organizations that process between 20,000 and 1 million transactions, while Level 4 applies to smaller merchants that process less than 20,000 transactions. PCI-DSS has six major control objectives. It requires the merchant to (a) build and maintain a secure network, (b) protect cardholder data, (c) maintain a vulnerability management program, (d) implement strong access control measures, (e) regularly test and monitor networks, and (f) maintain an information security policy. Each of these six broad control objectives has further specific requirements that must be met. The most current version of PCI-DSS is Version 3.1, which went into effect as of April 2015 (PCI Security Standards Council, 2015).

Limitations of Online Credit Card Payment Systems

There are a number of limitations to the existing credit card payment system. The most important limitations involve security, merchant risk, administrative and transaction costs, and social equity.

The existing system offers poor security. Neither the merchant nor the consumer can be fully authenticated. The merchant could be a criminal organization designed to collect credit card numbers, and the consumer could be a thief using stolen or fraudulent cards. The risk facing merchants is high: consumers can repudiate charges even though the goods have been shipped or the product downloaded. The banking industry attempted to develop a secure electronic transaction (SET) protocol, but this effort failed because it was too complex for consumers and merchants alike. The rate of online credit card fraud is expected to reach $4 billion in 2016, up from $2 billion in 2011. As banks switch to EMV cards with computer chips, offline credit card fraud becomes more difficult, encouraging criminals to focus on online fraud (Sidel, 2016).

The administrative costs of setting up an online credit card system and becoming authorized to accept credit cards are high. Transaction costs for merchants also are significant—roughly 3% of the purchase plus a transaction fee of 20–35 cents per transaction, plus other setup fees.

Credit cards are not very democratic, even though they seem ubiquitous. Millions of young adults do not have credit cards, along with almost 100 million other adult Americans who cannot afford cards or who are considered poor risks because of low incomes.

ALTERNATIVE ONLINE PAYMENT SYSTEMS

The limitations of the online credit card system have opened the way for the development of a number of alternative online payment systems. Chief among them is PayPal. PayPal (purchased by eBay in 2002 and then spun-off as an independent company again in 2015) enables individuals and businesses with e-mail accounts to make and receive payments up to a specified limit. Paypal is an example of an **online stored value payment system**, which permits consumers to make online payments to merchants and other individuals using their bank account or credit/debit cards. It is available in 202 countries and 25 currencies around the world. PayPal builds on the existing financial infrastructure of the countries in which it operates. You establish a PayPal account by specifying a credit, debit, or checking account you wish to have charged or paid when conducting online transactions. When you make a payment

online stored value payment system permits consumers to make instant, online payments to merchants and other individuals based on value stored in an online account

using PayPal, you e-mail the payment to the merchant's PayPal account. PayPal transfers the amount from your credit or checking account to the merchant's bank account. The beauty of PayPal is that no personal credit information has to be shared among the users, and the service can be used by individuals to pay one another even in small amounts. However, one issue with PayPal is its relatively high cost. For example, when using a credit card as the source of funds, to send or request money, the cost ranges from 2.9% to 5.99% of the amount (depending on the type of transaction) plus a small fixed fee (typically $0.30) per transaction. PayPal is discussed in further depth in the case study at the end of the chapter.

Although PayPal is by far the most well-known and commonly used online credit/debit card alternative, there are a number of other alternatives as well. Pay with Amazon is aimed at consumers who have concerns about entrusting their credit card information to unfamiliar online retailers. Consumers can purchase goods and services at non-Amazon websites using the payment methods stored in their Amazon accounts, without having to reenter their payment information at the merchant's site. Amazon provides the payment processing. Visa Checkout (formerly V.me) and MasterCard's MasterPass substitute a user name and password for an actual payment card number during online checkout. Both MasterPass and Visa Checkout are supported by a number of large payment processors and online retailers. However, they have not yet achieved the usage of Paypal.

Bill Me Later (owned by PayPal as well) also appeals to consumers who do not wish to enter their credit card information online. Bill Me Later describes itself as an open-ended credit account. Users select the Bill Me Later option at checkout and are asked to provide their birth date and the last four digits of their social security number. They are then billed for the purchase by Bill Me Later within 10 to 14 days. Bill Me Later is currently offered by more than 1,000 online merchants.

WU Pay (formerly eBillme, and now operated by Western Union) offers a similar service. WU Pay customers who select the WU Pay option at firms such as Sears, Kmart, and other retailers do not have to provide any credit card information. Instead they are e-mailed a bill, which they can pay via their bank's online bill payment service, or in person at any Western Union location. Dwolla is a similar cash-based payment network for both individuals and merchants. It bypasses the credit card network and instead connects directly into a bank account. In 2015, Dwolla eliminated its transaction and processing fees, changing its focus from consumer-to-consumer payments to larger businesses. Dwolla has its own network that bypasses the Automated Clearing House (ACH), the traditional system for processing financial transactions in the United States, and in 2015, signed up major U.S. bank BBVA Compass. Earlier in the year, the U.S. Treasury had selected Dwolla (along with PayPal) to process payments to federal agencies, and in October 2015, the Chicago Mercantile Exchange chose Dwolla to replace ACH. Dwolla now processes nearly $2 billion a year and has over 1 million accounts (Pendell, 2016; Patane, 2015; Leising, 2015).

Like Dwolla, Stripe is another company that is attempting to provide an alternative to the traditional online credit card system. Stripe focuses on the merchant side of the process. It provides simple software code that enables companies to bypass much of the administrative costs involved in setting up an online credit card system,

and instead lets companies begin accepting credit card payments almost immediately without the need to obtain a merchant account or use a gateway provider. Stripe recently introduced merchant apps that can accept NFC payments. Unlike PayPal, the customer doesn't need a Stripe account to pay, and all payments are made directly to the company rather than being routed through a third party.

MOBILE PAYMENT SYSTEMS: YOUR SMARTPHONE WALLET

The use of mobile devices as payment mechanisms is already well established in Europe and Asia and is now exploding in the United States, where the infrastructure to support mobile payment is finally being put in place.

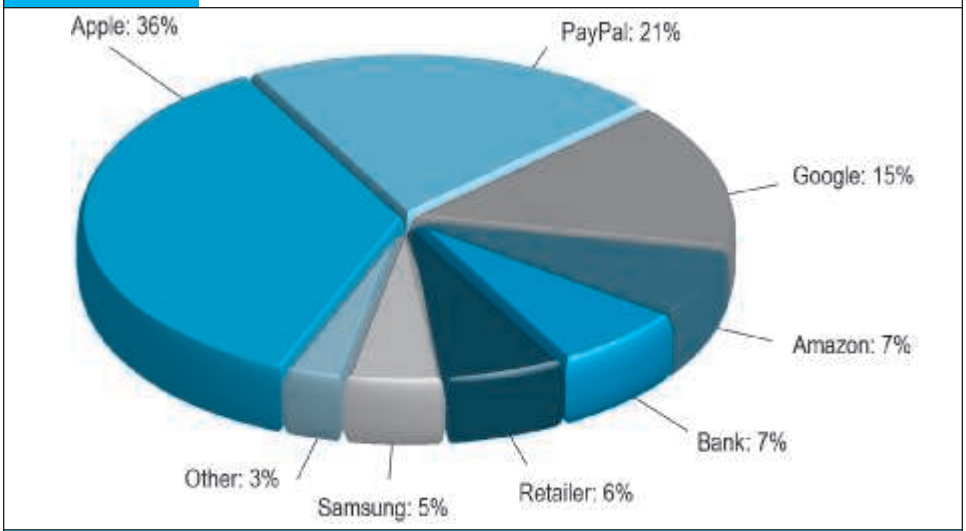
Near field communication (NFC) is the primary enabling technology for mobile payment systems. **Near field communication (NFC)** is a set of short-range wireless technologies used to share information among devices within about 2 inches of each other (50 mm). NFC devices are either powered or passive. A connection requires one powered device (the initiator, such as a smartphone), and one target device, such as a merchant NFC reader, that can respond to requests from the initiator. NFC targets can be very simple forms such as tags, stickers, key fobs, or readers. NFC peer-to-peer communication is possible where both devices are powered. Consumers can swipe their NFC-equipped phone near a merchant's reader to pay for purchases. In September 2014, Apple introduced the iPhone 6, which is equipped with NFC chips designed to work with Apple's mobile payments platform, Apple Pay. Building on Apple Passbook and Touch ID biometric fingerprint scanning and encryption that Apple previously introduced in September 2012, Apple Pay is able to be used for mobile payments at the point-of-sale at a physical store as well as online purchases using an iPhone. Other competitors in NFC-enabled mobile payments include Android Pay, Samsung Pay, PayPal, and Square. Surveys reveal that about 20%–30% of smartphone users have downloaded mobile wallet apps, but that only about 20% of these adopters have made a payment in the last month using these apps. **Figure 5.15** shows that Apple and PayPal are the most widely used mobile payment apps among adopters of mobile wallets. The promise of riches beyond description to a firm that is able to dominate the mobile payments marketplace has set off what one commentator has called a goat rodeo surrounding the development of new technologies and methods of mobile payment. The end-of-chapter case study, *Mobile Payment Marketplace: Goat Rodeo,* provides a further look at the future of online and mobile payment in the United States, including the efforts of Apple, Google, Samsung, Square, PayPal, and major financial institutions.

near field communication (NFC) a set of short-range wireless technologies used to share information among devices

SOCIAL/MOBILE PEER-TO-PEER PAYMENT SYSTEMS

In addition to using a mobile device as a vehicle for e-commerce and as a payment method at physical point-of-sale, another type of mobile payment transaction is becoming increasingly popular: social/mobile peer-to-peer payments. Services such as Venmo, Square Cash, Snapcash, the newly refocused Google Wallet, and the new Facebook Messenger Payment service all enable users to send another person money through a mobile application or website, funded by a bank debit card. There is no charge for this service. Currently, these services are the most popular among Millennials, which is the key demographic driving their growth. Venmo, owned by PayPal,

FIGURE 5.15 MOBILE WALLET ADOPTION



Apple Pay and PayPal's mobile wallet are the most widely used methods of mobile payment.
SOURCE: Based on data from eMarketer, Inc., 2016b.

is particularly popular, with its success in part due to its integration with Facebook and its social network newsfeed, which lets users see when friends are paying other friends or paying for products and services. In 2015, Venmo processed an estimated $8 billion in transactions and is growing at over 200% annually. In 2016, Facebook and PayPal announced that Facebook subscribers could use PayPal to purchase goods and services, with notifications coming through Facebook Messenger. Analysts forecast that mobile P2P will grow to $174 billion, worth 30% of total P2P payment volume, by 2020. That's up from $5.6 billion, or just 1%, in 2014 (BI Intelligence, 2016).

REGULATION OF MOBILE WALLETS AND RECHARGEABLE CARDS

In October 2016, the Bureau of Consumer Financial Protection (BCFP), a federal regulatory agency, issued the first regulations on what it called General Purpose Reloadable (GPR) cards. The regulations apply to some mobile digital wallets and to physical cards that can be loaded with prepaid funds, as well as cards that can be purchased at retail locations or recharged with funds at a bank ATM or merchant point-of-sale terminal (but not to gift cards purchased at retail locations). Previously, GPR cards were not subject to existing federal consumer banking regulations that provide protection from unauthorized transfers and require disclosure with respect to their terms and error resolution procedures. The BCFP estimates that GPR transactions grew from $1 billion in 2003 to $65 billion in 2012, with a projected growth to $117 billion in 2019 (BCFP, 2016). Physical GPR cards are generally sold to people who do not have a bank or credit account, and who use them as a substitute for a checking account and cash for mobile payments. Mobile digital wallets, in comparison, are typically used by people who already have these banking credentials. Venmo and similar peer-to-peer payment

services, as well as Android Pay and Samsung Pay, are subject to these regulations because they allow for the storage of prepaid funds. Apple Pay and similar wallets are not subject to these regulations because they do not store prepaid funds and simply act as an intermediary between the banks and consumers using existing bank credentials.

The new regulations require disclosure of financial terms to consumers prior to and after acquisition of a prepaid account, access to periodical statements, a means for consumers to correct errors in payments, consumer opt-in for over-draft and credit features, and a 21-day minimum repayment period. The regulations prohibit requiring customers to set up preauthorized electronic fund transfers to repay credit extended through an overdraft service or credit feature. These requirements are extensions of the existing Electronic Funds Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z) that apply to products of bank and credit institutions such as credit and debit cards.

DIGITAL CASH AND VIRTUAL CURRENCIES

Although the terms digital cash and virtual currencies are often used synonymously, they actually refer to two separate types of alternative payment systems. **Digital cash** typically is based on an algorithm that generates unique authenticated tokens representing cash value that can be used "in the real world." Bitcoin is the best known example of digital cash. Bitcoins are encrypted numbers (sometimes referred to as cryptocurrency) that are generated by a complex algorithm using a peer-to-peer network in a process referred to as "mining" that requires extensive computing power. Like real currency, Bitcoins have a fluctuating value tied to open-market trading. Like cash, Bitcoins are anonymous—they are exchanged via a 34-character alphanumeric address that the user has, and do not require any other identifying information. Bitcoins have recently attracted a lot of attention as a potential money laundering tool for cybercriminals and illicit drug markets like Silk Road, and have also been plagued by security issues, with some high-profile heists. Nonetheless, there are companies now using Bitcoins as a legitimate alternative payment system. Read the *Insight on Business* case, *Bitcoin*, for a further look at Bitcoin and some of the issues surrounding it.

digital cash
an alternative payment system in which unique, authenticated tokens represent cash value

Virtual currencies, on the other hand, typically circulate primarily within an internal virtual world community, such as Linden Dollars, created by Linden Lab for use in its virtual world, Second Life. Virtual currencies are typically used for purchasing virtual goods.

virtual currency
typically circulates within an internal virtual world community or is issued by a specific corporate entity, and used to purchase virtual goods

5.6 ELECTRONIC BILLING PRESENTMENT AND PAYMENT

In 2007, for the first time, the number of bill payments made online exceeded the number of physical checks written (Fiserv, 2007). In the $19 trillion U.S. economy with a $13.3 trillion consumer sector for goods and services, there are billions of bills to pay. According to the U.S. Postal Service, U.S. households received about 21 billion bills in 2015 via the mail. No one knows for sure, but some experts believe the life-cycle cost of a paper bill for a business, from point of issuance to point of payment, ranges from $3 to $7. This calculation does not include the value of time to consumers, who must open bills, read them, write checks, address envelopes, stamp, and then mail remit-

In this chapter, we discuss social networks, auctions, and portals. What do social networks, auctions, and portals have in common? They are all based on feelings of shared interest and self-identification—in short, a sense of community. Social networks and online communities explicitly attract people with shared affinities, such as ethnicity, gender, religion, and political views, or shared interests, such as hobbies, sports, and vacations. The auction site eBay started as a community of people interested in trading unwanted but functional items for which there was no ready commercial market. That community turned out to be huge—much larger than anyone expected. Portals also contain strong elements of community by providing access to community-fostering technologies such as e-mail, chat groups, bulletin boards, and discussion forums.

11.1 SOCIAL NETWORKS AND ONLINE COMMUNITIES

The Internet was designed originally as a communications medium to connect scientists in computer science departments around the continental United States. From the beginning, the Internet was intended, in part, as a community-building technology that would allow scientists to share data, knowledge, and opinions in a real-time online environment (see Chapter 3) (Hiltzik, 1999). The result of this early Internet was the first "virtual communities" (Rheingold, 1993). As the Internet grew in the late 1980s to include scientists from many disciplines and university campuses, thousands of virtual communities sprang up among small groups of scientists in very different disciplines that communicated regularly using Internet e-mail, listservs, and bulletin boards. The first articles and books on the new electronic communities began appearing in the mid- to late 1980s (Kiesler et al., 1984; Kiesler, 1986). One of the earliest online communities, The Well (originally Whole Earth 'Lectronic Link), was formed in San Francisco in 1985 by a small group of people who once shared an 1,800-acre commune in Tennessee. The Well continues to have thousands of members devoted to discussion, debate, advice, and help (Hafner, 1997; Rheingold, 1998). With the development of the Web in the early 1990s, millions of people began obtaining Internet accounts and e-mail, and the community-building impact of the Internet strengthened. By the late 1990s, the commercial value of online communities was recognized as a potential new business model (Hagel and Armstrong, 1997).

The early online communities involved a relatively small number of web aficionados, and users with intense interests in technology, politics, literature, and ideas. The technology was largely limited to posting text messages on bulletin boards sponsored by the community, and one-to-one or one-to-many e-mails. In addition to The Well, early networks included GeoCities, a website hosting service based on neighborhoods. By 2002, however, the nature of online communities had begun to change. User-created websites called blogs became inexpensive and easy to set up without any technical expertise. Photo sites enabled convenient sharing of photos. Beginning in 2007, the growth of mobile devices like smartphones, tablet computers, digital cameras, and portable media devices

enabled sharing of rich media such as photos, music, and videos. Suddenly there was a much wider audience for sharing interests and activities, and much more to share.

A new culture emerged as well. The broad democratization of the technology and its spread to the larger population meant that online social networks were no longer limited to a small group but instead broadened to include a much wider set of people and tastes, especially pre-teens, teens, and college students who were the fastest to adopt many of these new technologies. Entire families and friendship networks soon joined. The new social network culture is very personal and "me" centered, displaying photos and broadcasting personal activities, interests, hobbies, and relationships on social network profiles. In an online social network, the "news" is not something that happened somewhere else to other people; instead, the news is what happened to you today, and what's going on with your friends and colleagues. Today's social networks are as much a sociological phenomenon as they are a technology phenomenon.

Currently, social network participation is one of the most common usages of the Internet. Over three-quarters of all Internet users and about 70% of the total U.S. population—about 186 million Americans—use social networks (eMarketer, Inc., 2016a). Facebook has over 1.7 billion active users (with about 167 million in North America) and a little over 1.5 billion mobile monthly users (Facebook, 2016). There is obviously an overlap between these two sets of users. In the United States, Facebook typically has around 144 mobile users (again, with many of these being overlapping) (eMarketer, Inc., 2016b). Other large social networks include LinkedIn (profiled in the opening case), Twitter, Pinterest, Instagram, Snapchat, and Tumblr. While Facebook is the most popular social network in the United States, it is also the slowest growing, up just a few percentage points since 2012. Facebook appears to have hit a plateau in the United States, and its real hope for growth is offshore, where it is pushing to create basic Internet access so more people will join the network. Newer social networks, such as Pinterest, Instagram, and Snapchat, are growing much more quickly.

Worldwide, the social network phenomena is even stronger with over 2.3 billion users worldwide, 32% of the world's population, and still growing at 9% annually. Social networks are a top online destination in every country, accounting for the majority of time spent online, and reaching almost 79% of active Internet users. Asia-Pacific has the largest social network audience, followed by the Middle East and Africa, and Latin America, while North America has the highest penetration of social network usage among the general population (eMarketer, Inc., 2016c). Although Facebook dominates the global social network marketspace, in some countries, localized social networks are signficant, such as Orkut (owned by Google) in Brazil, Mixi and social messaging app Line in Japan, Qzone, QQ, Sina Weibo, and RenRen in China, XING in Germany, Tuenti in Spain, and VK in Russia. There is an online social network for you to join almost anywhere you go!

WHAT IS AN ONLINE SOCIAL NETWORK?

social network
involves a group of people, shared social interaction, common ties among members, and people who share an area for some period of time

So exactly how do we define an online social network, and how is it any different from, say, an offline social network? Sociologists, who frequently criticize modern society for having destroyed traditional communities, unfortunately have not given us very good definitions of social networks and community. One study examined 94 different sociological definitions of community and found four areas of agreement. **Social networks** involve (a) a group of people, (b) shared social interaction, (c) common ties

among members, and (d) people who share an area for some period of time (Hillery, 1955). This will be our working definition of a social network. Social networks do not necessarily have shared goals, purposes, or intentions. Indeed, social networks can be places where people just "hang out," share space, and communicate.

It's a short step to defining an **online social network** as an online location where people who share common ties can interact with one another. This definition is very close to that of Howard Rheingold's—one of The Well's early participants—who coined the term *virtual communities* as "cultural aggregations that emerge when enough people bump into each other often enough in cyberspace." It is a group of people who may or may not meet one another face to face, and who exchange words and ideas through the mediation of an online social meeting space. The Internet removes the geographic and time limitations of offline social networks. To be in an online network, you don't need to meet face to face, in a common room, at a common time.

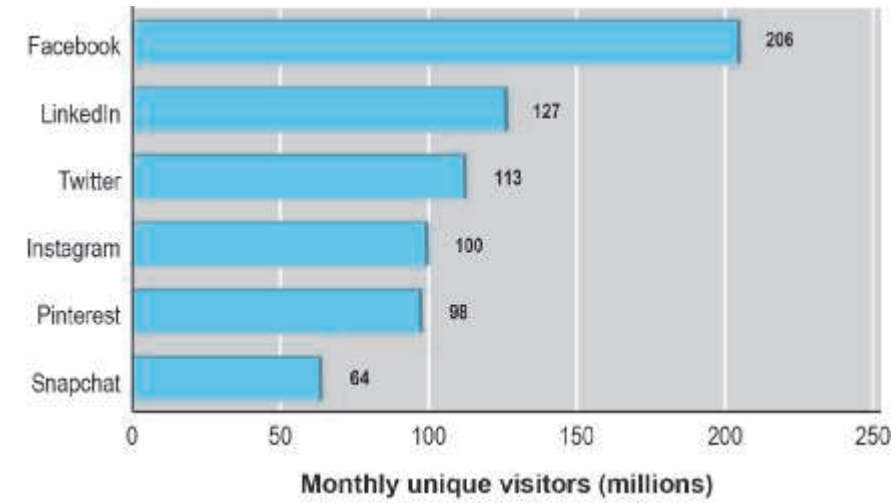
online social network an area online, where people who share common ties can interact with one another

THE GROWTH OF SOCIAL NETWORKS AND ONLINE COMMUNITIES

Figure 11.1 shows the top social networks, which together account for well over 90% of the Internet's social network activity.

The largest group of Facebook users in the United States are 25 to 34 years old (36 million), followed by 35- to 45-year-olds (30 million). Over one-third (35%) of U.S. Facebook users are older than 44. Adults over 65 constitute the fastest growing group on Facebook (eMarketer, Inc., 2016d). In contrast, Twitter is far more popular among young adults under 34. Similar patterns are observed worldwide as older populations use social networks to stay in touch with children and relatives. Facebook is the most popular social network among teens, with Instagram and Snapchat not far behind.

FIGURE 11.1 TOP U.S. SOCIAL NETWORKS 2016



Facebook is by far and away the dominant social network in the United States in terms of monthly unique visitors.

SOURCES: Based on data from comScore, 2016a; Instagram, 2016.

Newer social networks tend to follow this same pattern, with young people being the first adopters.

While Facebook and Twitter still tend to dominate the news, a new kind of social network is appearing and growing much faster than Facebook with respect to unique visitors and subscribers. These new social networks are attracting marketers and advertisers as well. For instance, Pinterest, described in the closing case in Chapter 1, is a visually oriented site that allows users to curate their tastes and preferences, expressed in visual arts. You can think of Pinterest as a visual blog. Users post images to an online "pinboard." The images can come from any source. Users can also "re-pin" images they see on Pinterest. Pinterest's membership has skyrocketed since its launch, accumulating 150 million active members worldwide as of October 2016. Instagram is another social network that focuses on video and photo sharing. A mobile app that enables a user to easily share images to social networks, Instagram was acquired by Facebook for $1 billion in 2012 and has over 500 million members in September 2016.

Other social networks are not necessarily competing with Facebook, but adding to the social network mix and enlarging the total social network audience. **Table 11.1** describes some other popular social networks.

Contributing to the continued growth and commercial success of networks is the rapid adoption and intense use of mobile devices. Over 90% of Facebook's users worldwide are mobile users, although not exclusively. According to comScore, Facebook's flagship Facebook app has the highest number of unique visitors (150 million) of all mobile apps and appears on the home screen of 46% of all smartphone users, with the average person spending 13 hours on the app a month (comScore, 2016b). Several of the largest newer social networks like Instagram and Snapchat are almost entirely mobile.

A new crop of social networks launched since 2008 focuses on messaging. Snapchat (2009) lets users send photos and videos to friends that self-extinguish in ten seconds. Snapchat Stories have a longer lifespan: 24 hours. Snapchat has very high reach among its core audience of 18- to 24-year-olds, but in 2016, it also began to break into the mainstream, with significant growth in the over-25 age group demographic (comScore, 2016b). WhatsApp (2009; acquired by Facebook in 2014) is a messaging service that lets users send text, photos, and videos to their friends' cellphones using the Internet and without having to pay telecommunications companies for cellphone SMS messaging services. Six of the world's most-used apps are messaging services.

The number of unique visitors is just one way to measure the influence of a site. Time on site is another important metric. The more time people spend on a site, called engagement, the more time to display ads and generate revenue. In this sense, Facebook is much more addictive and immersive than the other top social networks. Over time, Facebook has tweaked its content and algorithms in order to keep users on the site longer. In 2014, Facebook added videos (both ads and user-contributed), and in 2016 is now displaying around 8 billion videos a day. It tries to show videos that reflect the user's interests and friends and also plays them automatically in the News Feed, forcing users to turn them off but also ensuring that they are seen for at

TABLE 11.1 OTHER SOCIAL NETWORKS

SOCIAL NETWORK	DESCRIPTION
Myspace	Early leader in social networking was overtaken by Facebook; being reinvented as a music-oriented social network by pop star Justin Timberlake.
Meetup	Helps groups of people with shared interests plan events and meet offline.
Tagged	A network aimed at introducing members to one another through games, shared interests, friend suggestions, and browsing profiles.
MeetMe	Another social network aimed at meeting new people.
Polyvore	Topic-focused social network (fashion).
deviantART	Website focused on art, sharing of images.
Vevo	Video and music sharing site.

least a few moments. Facebook has also made changes to its News Feed algorithm to capture more user attention: increasing content from users' favorite friends; decreasing content from friends of users' friends; and showing multiple posts in a row from the same source for users with few friends (Gaudin, 2015). **Table 11.2** illustrates the different levels of engagement with the top social networks.

The amount of revenue generated is the ultimate metric for measuring a company's business potential. The top three search engine companies (Google, Yahoo, and Microsoft) are expected to generate about $30 billion in U.S. search and display advertising revenue in 2016 (eMarketer, Inc., 2016e). In contrast, social networks in

TABLE 11.2 TIME SPENT ON TOP SOCIAL NETWORKS

WEB SITE	MINUTES/MONTH (IN BILLIONS)
Facebook	230
Instagram	12.2
Twitter	6.6
Pinterest	6.5
Snapchat	6.4
Tumblr	5.0
LinkedIn	1.7

SOURCES: Based on data from comScore, 2015.

the United States in 2016 are expected to generate about $15.4 billion in advertising revenue. Social networks are the fastest growing form of Internet usage and advertising revenue, but they are not yet as lucrative as traditional search engines/portals in terms of ad dollars generated. A part of the problem is that subscribers do not go to social networks to seek ads for relevant products, nor pay attention to the ads that are flashed before their eyes (see Chapters 6 and 7). In addition, the small screen of the smartphone, the dominant social network platform, is not ideal for display advertising of retail goods. Here, tablets and desktop PCs are more suitable for browsing and purchasing.

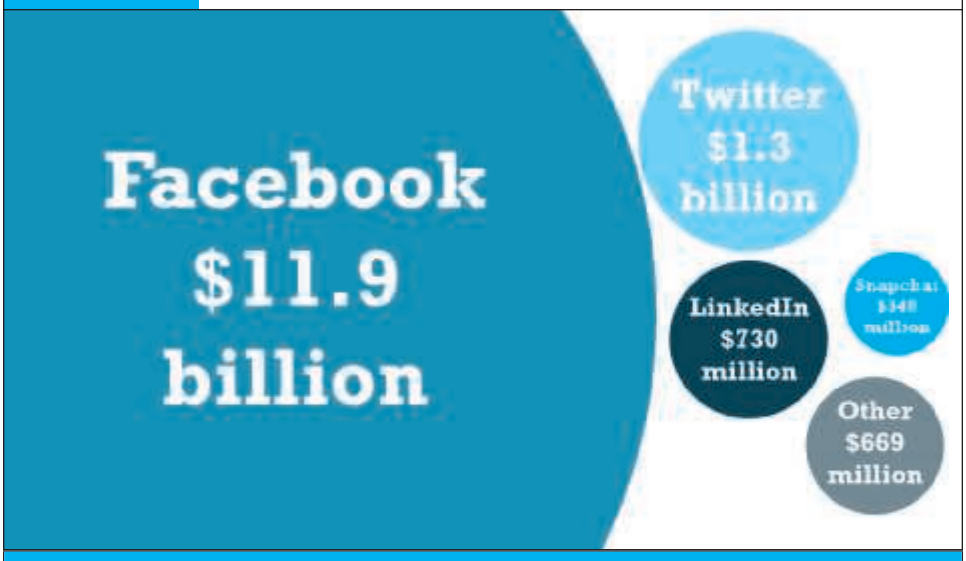
TURNING SOCIAL NETWORKS INTO BUSINESSES

While the early social networks had a difficult time raising capital and revenues, today's top social networks are now monetizing their huge audiences. Early social networks relied on subscriptions, but today, most social networks rely on advertising or the investments of venture capitalists. Users of portals and search engines have come to accept advertising as the preferred means of supporting web experiences rather than paying for it. One important exception is LinkedIn, which offers basic free memberships for individuals but charges for premium services. **Figure 11.2** shows the comparative amount of ad spending on various social networks. Facebook, with almost $12 billion in ad revenue, towers over the other sites.

Social networks do not always succeed as businesses. For instance, Twitter began as a social messaging service on which users could communicate with followers. It quickly turned into an Internet broadcasting network for millions of on-scene observers acting as citizen reporters, as well as political organizers, celebrities, and politicians. In 2016, it has just over 300 million users. Twitter's growth has stagnated, and in 2015, it lost $521 million, disappointing investors who expect more advertising dollars and real revenue. Twitter has never shown a profit. In 2015, co-founder Jack Dorsey returned in October 2015 in an effort to reinvigorate Twitter's user and revenue growth. But despite a number of incremental changes designed to streamline the service and make it easier to use, as well as several new strategic efforts, such as live-streaming video partnerships with the sports leagues like the NFL, Twitter's share of U.S. social networks has continued to drop. In September 2016, Twitter is reportedly up for sale. See the Chapter 2 opening case on Twitter for a more detailed discussion of Twitter's business model.

The rapid adoption of mobile devices initially posed a challenge to social networks like Facebook, as well as Google's search engine, because they were largely based on the desktop platform. Google dominated mobile ad revenues up until 2013 because its search engine and Google Maps were among the most popular apps. Facebook quickly developed its own mobile app, and purchased others, and within the space of four years has been able to capture a significant part of the mobile ad market, using its mobile News Feed to provide users a continual stream of ads. The top seven apps, and eight of the top nine, are owned by either Google or Facebook. For Facebook, that includes the main Facebook app (1st), Facebook Messenger (2nd), and Instagram (9th). Today, around 85% of Facebook's revenue (around $10.1 billion) comes from mobile

FIGURE 11.2 U.S. AD SPENDING ON SOCIAL NETWORKS, 2016



SOURCE: Based on data from eMarketer, 2016f.

advertising. Other social network apps within the top 25 are Snapchat (13th), Pinterest (14th), and Twitter (17th) (comScore, 2016b).

Social networks have had an important impact on how businesses operate, communicate, and serve their customers. A 2015 survey of Fortune 500 firms found that 93% used LinkedIn, 78% used Twitter, and 74% used Facebook (Barnes et al., 2015). The most visible business firm use of social networks is as a marketing and branding tool. A less visible marketing use of networks is as a powerful listening tool that has strengthened the role of customers and customer feedback systems inside a business. Public social networks like Facebook have not been used extensively in firms as collaboration tools thus far. However, in 2015, Facebook launched its Facebook at Work app, designed to spur collaboration and networking inside large firms, as a pilot project. In October 2016, it finally released the commercial version of the app, now called Workplace. The new app faces stiff competition from a wide array of collaboration tools provided by Cisco, Microsoft, IBM, and along with other technologies like instant messaging and teleconferencing.

Social networks are where corporate brands and reputations are formed, and firms today take very seriously the topic of "online reputation," as evidenced by social network posts, commentary, chat sessions, and Likes. In this sense, social networks become an extension of corporate customer relationship management systems and extend existing market research programs. Beyond branding, social networks are being used increasingly as advertising platforms to contact a younger audience than websites and e-mail, and as customers increasingly shift their eyeballs to social networks. Rosetta Stone, for instance, uses its Facebook page to display videos of its learning technology, encourage discussions and reviews, and post changes in its learning tools. Yet the business

use of social networks does not always go well. The *Insight on Society* case, *The Dark Side of Social Networks*, discusses some of the risks associated with social networks.

TYPES OF SOCIAL NETWORKS AND THEIR BUSINESS MODELS

There are many types and many ways of classifying social networks and online communities. While the most popular general social networks have adopted an advertising model, other kinds of networks have different revenue sources. Social networks have different types of sponsors and different kinds of members. For instance, some are created by firms such as IBM for the exclusive use of their sales force or other employees (intra-firm communities or B2E [business-to-employee] communities); others are built for suppliers and resellers (inter-organizational or B2B communities); and others are built by dedicated individuals for other similar persons with shared interests (P2P [people-to-people] communities). In this chapter, we will discuss B2C communities for the most part, although we also discuss briefly P2P communities of practice.

Table 11.3 describes in greater detail the five generic types of social networks and online communities: general, practice, interest, affinity, and sponsored. Each type of community can have a commercial intent or commercial consequence. We use this schema to explore the business models of commercial communities.

general communities offer members opportunities to interact with a general audience organized into general topics

General communities offer members opportunities to interact with a general audience organized into general topics. Within the topics, members can find hundreds of specific discussion groups attended by thousands of like-minded members who share an interest in that topic. The purpose of the general community is to attract enough members to populate a wide range of topics and discussion groups. The busi-

TABLE 11.3 TYPES OF SOCIAL NETWORKS AND ONLINE COMMUNITIES

TYPE OF SOCIAL NETWORK / COMMUNITY	DESCRIPTION
General	Online social gathering place to meet and socialize with friends, share content, schedules, and interests. Examples: Facebook, Pinterest, Instagram, Tumblr, and Twitter.
Practice	Social network of professionals and practitioners, creators of artifacts such as computer code or music. Examples: Just Plain Folks (musicians' community), LinkedIn (business), and Doximity (physicians and health care professionals).
Interest	Community built around a common interest, such as games, sports, music, stock markets, politics, health, finance, foreign affairs, or lifestyle. Examples: Debatepolitics.com (political discussion group) and PredictWallStreet (stock market site).
Affinity	Community of members who self-identify with a demographic or geographic category, such as women, African Americans, or Arab Americans. Examples: BlackPlanet (African American community and social network site) and Healthboards.com (focusing on women's health issues).
Sponsored	Network created by commercial, government, and nonprofit organizations for a variety of purposes. Examples: Nike, IBM, Cisco, and political candidates.

INSIGHT ON SOCIETY

THE DARK SIDE OF SOCIAL NETWORKS

In 2015, theme park chain SeaWorld thought it had a great marketing idea when it launched a Twitter hashtag campaign to improve its public image. Using the hashtag #AskSeaWorld, the company solicited questions from Twitter users in an attempt to be more transparent about its operations. SeaWorld is a frequent target for animal rights activists, who object to the company's treatment of sea animals, and was the subject of the 2013 documentary Blackfish, which told the story of a whale whose mistreatment and resulting erratic behavior led to the deaths of three people. After the documentary, SeaWorld's ticket sales plunged and its already spotty public image was devastated. The company hoped that the hashtag campaign would be a much needed step in its rehabilitation.

That's not exactly how the campaign turned out. First, People for the Ethical Treatment of Animals (PETA) used the hashtag to attack SeaWorld for its poor animal care. SeaWorld failed to respond. Soon, many more activists and regular people jumped on the bandwagon, relentlessly attacking SeaWorld and its animal handling techniques. Some users asked why the parking lots at SeaWorld are bigger than the whale tanks, for example.

Instead of demonstrating its awareness of the improvement it needs to make in these areas, SeaWorld finally answered these and other concerns by stating, "No time for bots and bullies. We want to answer your questions," completely dismissing its skeptics. The company posted several more tweets with crying babies and memes of Internet trolls to represent the animal rights activists. Needless to say, this only made things worse for SeaWorld. In 2016, well over a year later, angry animal lovers continue to use the hashtag to attack SeaWorld's treatment of whales, dolphins, and other marine animals. SeaWorld's stock price hit an all-time low in August 2016. By any measure, SeaWorld presented us with a textbook case in how social network advertising and branding can go horribly wrong.

Attempts at humor can also often go horribly awry, as Budweiser discovered in advertising for its Bud Light brand. The company introduced the hashtag #upforwhatever in 2015, supported by TV ads and advertising on other platforms. One of the 47 slogans that accompanied the hashtag on its beer bottles was "The perfect beer for removing 'no' from your vocabulary for the night." Many of Bud Light's followers were shocked that the company would make such a controversial statement. The company claimed that its slogans were intended to inspire spontaneous fun, but admitted that this particular slogan was a misfire and immediately apologized and discontinued its use.

Soft drink giant Coca-Cola also encountered the dark side of social networks after its 2016 campaign to wish its customers in different countries Happy New Year. First, the company sent a message on VK, the most popular Russian social network, consisting of a map of Russia decorated with holiday ornaments. There was nothing offensive about the decorations, but Coca-Cola omitted the disputed territory of Crimea. Russian followers of Coca-Cola were enraged. In response, Coca-Cola adjusted the map, adding the Crimea as well as other territories it had neglected the first time around. This time, it was Ukraine's turn to take offense. Ukraine and Russia have been battling over the area since 2014, and Ukrainians believe the territory has been unlawfully annexed by Russia. Many Ukrainians vowed to boycott Coca-Cola, with some tweeting pictures of themselves pouring Coke down the toilet in disgust. Coca-Cola eventually deleted the second image without replacing the first image.

The SeaWorld, Bud Light, and Coca-Cola fiascos are instructive. SeaWorld was totally unprepared for a hashtag campaign gone wrong. Bud Light didn't consider how its messaging might be

(continued)

interpreted as offensive by many customers. Coca-Cola failed to fully recognize the unique aspects of each geopolitical region in which it operates. Companies need to be prepared to handle negative comments appropriately and take responsibility for mistakes.

Companies don't appear to be learning from the earlier mistakes of their peers. For example, in 2014, homemade pizza maker DiGiorno's blundered when it used a hashtag meant to bring awareness to domestic violence, #WhyIStayed, in a tweet promoting its pizza. Outrage came swiftly and DiGiorno's took the tweet down amid a storm of criticism. The New England Patriots football team ran a campaign that automatically retweeted users' Twitter account names superimposed on team jerseys when users tweeted the #1MillionPatriots hashtag. Users seized the opportunity to wreak havoc, creating offensive Twitter handles that embarrassed the Patriots. And US Airways inadvertently tweeted a graphic pornographic image in response to a customer service complaint. Perhaps most surprisingly of all, Twitter's own chief financial officer accidentally publicly tweeted a message about an acquisition the company was still considering.

But in 2014, KFC set a good example when the news broke that a 3-year-old girl from Mississippi who had been mauled by her grandfather's dogs had subsequently been asked to leave a local KFC because she reportedly was scaring the other patrons. The visit to the restaurant had been a special treat for the girl from her family after a doctor's visit. When the news hit social media, KFC was caught in a firestorm of enraged customers. The company took the next several days to respond to as many individual comments as it could, posted a personal apology to the girl's Facebook page, and pledged $30,000 toward her medical bills.

Marketing is not the only social media hazard. For employees, privacy protection for Facebook posts is still being determined in the courts. For example, Danielle Mailhoit was the manager of a Home Depot store in Burbank, California. After she was fired, she filed suit claiming gender and disability discrimination due to her vertigo. The defense attorney filed a broad request for all of Mailhoit's social media activity. In September 2012, a federal judge ruled this request overly broad and limited discovery to only communications between the plaintiff and current or former Home Depot employees. Stating that they were unlikely to be relevant unless they were directly related to the lawsuit or her former employment, she also denied Home Depot's request for photos.

Employers must be careful with personal information gleaned from social networks. If it can be proven that membership in a protected group was discovered during the hiring process and used to reject a candidate or later used to terminate an employee, a claim can be filed under one of the Federal Equal Employment Opportunity (EEO) laws. These include Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act of 1967 (ADEA), Title I and Title V of the Americans with Disabilities Act of 1990 (ADA), and Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA), which prohibits employment discrimination based on genetic information about an applicant, employee, or former employee. GINA's regulations provide a distinction between whether genetic information is acquired purposefully or inadvertently. Inadvertent acquisition includes acquisition through social networks, equating it to accidentally overhearing a conversation at work.

However, data on a social media site protected by privacy controls should not be able to be "inadvertently" acquired. The Stored Communications Act (SCA) covers privacy protection for e-mail and digital communications. The latest court rulings on its application to social network communications have held that Facebook wall postings and other social media comments are protected as long as they have not been made public.

Facebook, to protect its business model, is speaking out against recent hiring practices that have come to its attention—and threatening legal action. According to both Facebook and the Ameri-

can Civil Liberties Union (ACLU), some companies have been asking new hires either to friend the hiring manager or to submit their password. Facebook's Privacy Page condemns this practice, stating that it violates both individual users' and their friends' expectations of privacy, jeopardizes security, and could reveal a user's membership in a protected group. The legal implications of interactions on social media are still being determined; for example, in 2016, a judge ruled that "tagging" someone in a photo represents the violation of a protective order limiting communication.

Legislators in a growing number of states have decided to be proactive. In 2012, California banned employers from asking prospective employees for their social media user names and passwords. In 2016, Illinois became the 25th state to enact a law that prevents employers from accessing potential employees' social media accounts, with Massachusetts and Ohio poised to add to that number in 2017. Additionally, 15 states have enacted laws that forbid educational institutions from doing so for their prospective students. At the federal level, the House passed a bill in 2016 that requires the President to submit a strategy to address the use of social media by terrorist groups.

Carefully crafted policies can help companies to avoid the dark side of social networking. Advertising and hiring are but two of the areas that must be monitored. Companies must also develop policies regarding employee use of social networks. Employee education programs must be implemented to apprise employees of infractions that can be grounds for disciplinary action. IT departments must develop stringent policies to protect proprietary data and defend company networks from cyberscams. Social networking is an exciting new tool, but one that requires safeguards.

SOURCES: "States Lock Up Social Media Access From Employers," by KSE Focus, Cqrollcall.com, September 7, 2016; "State Social Media Privacy Laws," Nscl.org, July 6, 2016; "Ernst-Backed Bill to Combat Terrorist Use of Social Media Passes Committee," Ernst.senate.gov, February 10, 2016; "Why Googling Candidates Before You Decide to Interview Them is Against the Law," by Diane Faulkner, Adp.com, February 4, 2016; Mariella Moon, "Judge Says Facebook Tagging Violates Protective Orders," Engadget.com, January 17, 2016; "The Top 10 Most Embarrassing Social Media Fails from 2015," by Carlos Matias, Socialmediaweek.org, January 5, 2016; "Top 5 Worst Social Media Brand Blunders of 2015," by Erin Carson, Techrepublic.com, December 18, 2015; "'Ask SeaWorld' Marketing Campaign Backfires," by Katie Lobosco,Cnnmoney.com, March 27, 2015; "Virginia's New Social Media Law Protects Employees," Troutmansanders.com, July 1, 2015; "The 5 Worst Twitter Marketing Fails of 2014," by Kim Lachance Shandrow, Entrepreneur.com, December 18, 2014; "10 Worst Social Media Fails of 2014," by Emily Alford, Clickz.com, December 18, 2014; "The Top 10 Social Media Fails of 2014," by Rebecca Borison, Inc.com, December 10, 2014; "RI Passes Social Media Privacy Law," by Bill Tomison, Wpri.com, July 3, 2014; "Facebook's Facing a Losing Battle to Protect Users' Privacy," by Lisa Vaas, Nakedsecurity.sophos.com, June 30, 2014; "KFC Shows How to Handle a Social Media Disaster," by Mary Elizabeth Williams, Salon.com, June 17, 2014; "The Dangers of Using Social Media Data in Hiring," by Gregg Skall, *Radio Business Report,* June 6, 2011; "Stored Communications Act Protects Facebook and MySpace Users' Private Communication," by Kathryn Freund, Jolt.law.harvard.edu, June 11, 2010.

ness model of general communities is typically advertising supported by selling ad space on pages and videos.

Practice networks offer members focused discussion groups, help, information, and knowledge relating to an area of shared practice. For instance, Linux.org is a nonprofit community for the open source movement, a worldwide global effort involving thousands of programmers who develop computer code for the Linux operating system and share the results freely with all. Other online communities involve artists, educators, art dealers, photographers, and nurses. Practice networks can be either profit-based or nonprofit, and support themselves by advertising or user donations.

Interest-based social networks offer members focused discussion groups based on a shared interest in some specific subject, such as business careers, boats, horses, health, skiing, and thousands of other topics. Because the audience for interest communities is necessarily much smaller and more targeted, these communities have usually relied on advertising and

practice networks
offer members focused discussion groups, help, information, and knowledge relating to an area of shared practice

interest-based social networks
offer members focused discussion groups based on a shared interest in some specific topic

tenancy/sponsorship deals. Social networks such as Fool.com, Military.com, Sailing Anarchy, and Chronicle Forums all are examples of social networks that attract people who share a common pursuit. Job markets and forums such as LinkedIn can be considered interest-based social networks as well.

affinity communities offer members focused discussions and interaction with other people who share the same affinity

Affinity communities offer members focused discussions and interaction with other people who share the same affinity. "Affinity" refers to self- and group identification. For instance, people can self-identify themselves on the basis of religion, ethnicity, gender, sexual orientation, political beliefs, geographical location, and hundreds of other categories. For instance, Bloom is a network for pregnant women and moms that enables them to give and seek advice, discuss concerns and share stories, as well as find local services, and buy and sell related products (Bloomapp.co, 2016). These social networks are supported by advertising along with revenues from sales of products.

sponsored communities online communities created for the purpose of pursuing organizational (and often commercial) goals

Sponsored communities are online communities created by government, nonprofit, or for-profit organizations for the purpose of pursuing organizational goals. These goals can be diverse, from increasing the information available to citizens; for instance, a local county government site such as Westchestergov.com, the website for Westchester County (New York) government; to an online auction site such as eBay; to a product site such as Tide.com, which is sponsored by an offline branded product company (Procter & Gamble). Cisco, IBM, HP, and hundreds of other companies have developed their internal corporate social networks as a way of sharing knowledge.

SOCIAL NETWORK TECHNOLOGIES AND FEATURES

algorithms set of step-by-step instructions, similar to a recipe, for producing a desired output from required inputs

computer algorithms computer programs that carry out step-by-step instructions to produce desired outputs

Algorithms are one of the most important technologies used by social networks. **Algorithms** are a set of step-by-step instructions, similar to a recipe, for producing a desired output from required inputs. **Computer algorithms** are computer programs that carry out step-by-step instructions to produce desired outputs (Coremen, et. al., 2009). Algorithms are an ancient concept, but are fundamental to how computers are used today to do everything from calculating pay checks, the amount you owe when purchasing online, selecting movies on Netflix that you are likely to watch, or recommending products you may be interested in based on your prior purchases. How, for instance, does Facebook decide what trending news to list in your Trending section, which of your posts to post on your friends' News Feeds, and which Instant Articles to make available on your mobile News Feed?

The problem Facebook and other social sites need to solve is how to select content (actions of their friends and news stories) for display on users' pages that they will find interesting, and likely click on. Also, Facebook needs to prevent information that is irrelevant from appearing on user pages. **Figure 11.3** illustrates the generic algorithm Facebook uses to produce what it calls relationship-based content personalized for members of a social network based on a patent it filed in 2010. It shows the generic eight steps in the algorithm (left column), and a translation of each step (right column). Facebook users organize themselves into affinity groups by selecting and accepting one another as friends. **Affinity groups** are a key concept here and in all social networks: they are generally composed of like-minded people who share views, attitudes, purchase patterns, and tastes in music and videos. Facebook attempts to discover exactly what those views, attitudes, purchase patterns, and tastes in music and videos

affinity groups generally composed of like-minded people who share views, attitudes, purchase patterns, and tastes in music and videos

11.2 ONLINE AUCTIONS

consumer-to-consumer (C2C) auctions
auction house acts as an intermediary market maker, providing a forum where consumers can discover prices and trade

Auctions are used throughout the e-commerce landscape. The most widely known auctions are **consumer-to-consumer (C2C) auctions**, in which the auction house is simply an intermediary market maker, providing a forum where consumers—buyers and sellers—can discover prices and trade. The market leader in C2C auctions is eBay, which, as of June 2016, had around 164 million active users in the United States and over 800 million items listed on any given day within thousands of different categories. In August 2016, eBay had around 110 million unique visitors, placing it 18th on the list of top 50 digital media (both desktop and mobile) properties (comScore, 2016a). In 2015, eBay had about $6.1 billion in net revenues from its Marketplaces segment, a 4% decline from 2014, and the total worth of goods sold or auctioned was around $78 billion, a 2% decline from 2014 (eBay, 2016). eBay is further discussed in the case study at the end of this chapter. In the United States alone, there are several hundred auction sites, some specializing in unique collectible products such as stamps and coins, others adopting a more generalist approach in which almost any good can be found for sale.

business-to-consumer (B2C) auctions
business sells goods it owns, or controls, using various dynamic pricing models

Less well known are **business-to-consumer (B2C) auctions**, where a business owns or controls assets and uses dynamic pricing to establish the price. Increasingly, online retail sites, such as Sam's Club, are adding auctions to their sites. Auctions also constitute a significant part of B2B e-commerce in 2016, and more than a third of procurement officers use auctions to procure goods.

Some leading online auction sites are listed in **Table 11.5**. Auctions are not limited to goods and services. They can also be used to allocate resources, and bundles of resources, among any group of bidders. For instance, if you wanted to establish an optimal schedule for assigned tasks in an office among a group of clerical workers, an auction in which workers bid for assignments would come close to producing a nearly optimal solution in a short amount of time (Parkes and Ungar, 2000). In short, auctions—like all markets—are ways of allocating resources among independent agents (bidders).

BENEFITS AND COSTS OF AUCTIONS

The Internet is primarily responsible for the resurgence in auctions. The Internet provides a global environment and very low fixed and operational costs for the aggregation of huge buyer audiences, composed of millions of consumers worldwide, who can use a universally available technology (Internet browsers) to shop for goods.

Benefits of Auctions

Aside from the sheer game-like fun of participating in auctions, consumers, merchants, and society as a whole derive a number of economic benefits from participating in Internet auctions. These benefits include:

- **Liquidity:** Sellers can find willing buyers, and buyers can find sellers. Sellers and buyers can be located anywhere around the globe. Just as important, buyers and

TABLE 11.5	LEADING ONLINE AUCTION SITES
GENERAL	
eBay	The world market leader in auctions: 110 million visitors a month and hundreds of millions of products.
eBid	In business since 1998. Operates in 23 countries, including the United States. Currently, one of the top competitors to eBay. Offers much lower fees.
uBid	Marketplace for excess inventory from pre-approved merchants.
OnlineAuction	Allows sellers to list for a low monthly fee, without a per-item listing or additional fees when the item sells.
SPECIALIZED	
Racersauction	Specialized site for automobile racing parts.
Philatelicphantasies	Stamp site for professionals, monthly online stamp auction.
Stacksbowers	America's largest fully automated auction company of certified coins including ancient gold, silver, and copper coins. Also offers sports cards.
Bid4Assets	Liquidation of distressed real estate assets from government and the public sector, corporations, restructurings, and bankruptcies.
Oldandsold	Online auction service specializing in quality antiques. Dealers pay a 3% commission on merchandise sold.
B2C AUCTIONS	
Auctions.samsclub	Merchandise from Sam's Club in a variety of categories.
Shopgoodwill	Goodwill's online auction site. Offers a wide variety of collectibles, books, and antiques chosen from the goods donated to Goodwill.

sellers can find a global market for rare items that would not have existed before the Internet.

- **Price discovery:** Buyers and sellers can quickly and efficiently develop prices for items that are difficult to assess, where the price depends on demand and supply, and where the product is rare.
- **Price transparency:** Public Internet auctions allow everyone in the world to see the asking and bidding prices for items.
- **Market efficiency:** Auctions can, and often do, lead to reduced prices, and hence reduced profits for merchants, leading to an increase in consumer welfare—one measure of market efficiency.
- **Lower transaction costs:** Online auctions can lower the cost of selling and purchasing products, benefiting both merchants and consumers. Like other Internet markets, such as retail markets, Internet auctions have very low (but not zero) transaction costs.
- **Consumer aggregation:** Sellers benefit from large auction sites' ability to aggregate a large number of consumers who are motivated to purchase something in one marketspace.

- **Network effects:** The larger an auction site becomes in terms of visitors and products for sale, the more valuable it becomes as a marketplace for everyone by providing liquidity and several other benefits listed previously, such as lower transaction costs, higher efficiency, and better price transparency.

Risks and Costs of Auctions

There are a number of risks and costs involved in participating in auctions. In some cases, auction markets can fail—like all markets at times. (We describe auction market failure in more detail later.) Some of the more important risks and costs to keep in mind are:

- **Delayed consumption costs:** Internet auctions can go on for days, and shipping will take additional time.
- **Monitoring costs:** Participation in auctions requires your time to monitor bidding.
- **Equipment costs:** Internet auctions require you to purchase a computer system and pay for Internet access.
- **Trust risks:** Online auctions are a significant source of Internet fraud. Using auctions increases the risk of experiencing a loss.
- **Fulfillment costs:** Typically, the buyer pays fulfillment costs of packing, shipping, and insurance, whereas at a physical store these costs are included in the retail price.

Auction sites such as eBay have taken a number of steps to reduce consumer participation costs and trust risk. For instance, auction sites attempt to solve the trust problem by providing a rating system in which previous customers rate sellers based on their overall experience with the merchant. Although helpful, this solution does not always work. Auction fraud is a leading source of e-commerce complaints to federal law enforcement officials. Another partial solution to high monitoring costs is, ironically, fixed pricing. At eBay, consumers can reduce the cost of monitoring and waiting for auctions to end by simply clicking on the Buy It Now button and paying a premium price. The difference between the Buy It Now price and the auction price is the cost of monitoring.

Nevertheless, given the costs of participating in online auctions, the generally lower cost of goods on Internet auctions is in part a compensation for the other additional costs consumers experience. On the other hand, consumers experience lower search costs and transaction costs because there usually are no intermediaries (unless, of course, the seller is an online business operating on an auction site, in which case there is a middleman cost), and usually there are no local or state taxes.

Merchants face considerable risks and costs as well. At auctions, merchants may end up selling goods for prices far below what they might have achieved in conventional markets. Merchants also face risks of nonpayment, false bidding, bid rigging, monitoring, transaction fees charged by the auction site, credit card transaction processing fees, and the administration costs of entering price and product information.

AUCTIONS AS AN E-COMMERCE BUSINESS MODEL

Online auctions have been among the most successful business models in retail and B2B commerce. eBay, the Internet's most lucrative auction site, has been profitable nearly since its inception. The strategy for eBay has been to make money off every stage in

the auction cycle. eBay earns revenue from auctions in several ways: transaction fees based on the amount of the sale, listing fees for display of goods, financial service fees from payment systems such as PayPal, and advertising or placement fees where sellers pay extra for special services such as particular display or listing services. PayPal has been faster growing and more profitable than eBay's markets, growing to more than half of eBay's revenue. In 2015, eBay spun off PayPal into a separate company, and going forward will have to make its profits from its markets operation.

However, it is on the cost side that online auctions have extraordinary advantages over ordinary retail or catalog sites. Auction sites carry no inventory and do not perform any fulfillment activities—they need no warehouses, shipping, or logistical facilities. Sellers and consumers provide these services and bear these costs. In this sense, online auctions are an ideal digital business because they involve simply the transfer of information.

Even though eBay has been extraordinarily successful, the success of online auctions is qualified by the fact that the marketplace for online auctions is highly concentrated. eBay dominates the online auction market, followed by eBid and uBid. In the last several years eBay's growth has slowed considerably as consumers shift toward Buy It Now purchases rather than auctions. Many of the smaller auction sites are not profitable because they lack sufficient sellers and buyers to achieve liquidity. In auctions, network effects are highly influential, and the tendency is for one or two very large auction sites to dominate, with hundreds of smaller specialty auction sites (sites that sell specialized goods such as stamps) being barely profitable.

TYPES AND EXAMPLES OF AUCTIONS

The primary types of auctions found on the Internet are English auctions, Dutch Internet auctions, Name Your Own Price auctions, and so-called penny auctions.

English auction
most common form of auction; the highest bidder wins

The **English auction** is the easiest to understand and the most common form of auction on eBay. Typically, there is a single item up for sale from a single seller. There is a time limit when the auction ends, a reserve price below which the seller will not sell (usually secret), and a minimum incremental bid set. Multiple buyers bid against one another until the auction time limit is reached. The highest bidder wins the item (if the reserve price of the seller has been met or exceeded). English auctions are considered to be seller-biased because multiple buyers compete against one another—usually anonymously.

Dutch Internet auction
public ascending price, multiple unit auction. Final price is lowest successful bid, which sets price for all higher bidders

The **Dutch Internet auction** format is perfect for sellers that have many identical items to sell. Sellers start by listing a minimum price, or a starting bid for one item, and the number of items for sale. Bidders specify both a bid price and the quantity they want to buy. The uniform price reigns. Winning bidders pay the same price per item, which is the lowest successful bid. This market clearing price can be less than some bids. If there are more buyers than items, the earliest successful bids get the goods. In general, high bidders get the quantity they want at the lowest successful price, whereas low successful bidders might not get the quantity they want (but they will get something).

Name Your Own Price auction
auction where users specify what they are willing to pay for goods or services

The **Name Your Own Price auction** was pioneered by Priceline, and is the second most-popular auction format on the Web. Although Priceline also acts as an intermediary, buying blocks of airline tickets, hotel rooms, and vacation packages at

a discount and selling them at a reduced retail price or matching its inventory to bidders, it is best known for its Name Your Own Price auctions, in which users specify what they are willing to pay for goods or services, and multiple providers bid for their business. Prices do not descend and are fixed: the initial consumer offer is a commitment to purchase at that price. In 2015, Priceline had more than $9.2 billion in revenues, and in 2016, it attracts around 20 million unique visitors a month. It is one of the top-ranked travel sites in the United States.

But how can Priceline offer such steep discounts off prices for services provided by major brand-name providers? There are several answers. First, Priceline "shields the brand" by not publicizing the prices at which major brands sell. This reduces conflict with traditional channels, including direct sales. Second, the services being sold are perishable: if a Priceline customer did not pay something for the empty airline seat, rental car, or hotel room, sellers would not receive any revenue. Hence, sellers are highly motivated to at least cover the costs of their services by selling in a spot market at very low prices. The strategy for sellers is to sell as much as possible through more profitable channels and then unload excess capacity on spot markets such as Priceline. This works to the advantage of consumers, sellers, and Priceline, which charges a transaction fee to sellers.

penny (bidding fee) auction
bidder must pay a non-refundable fee to purchase bids

So-called penny auctions are really anything but. To participate in a **penny auction** (also known as a **bidding fee auction**), you typically must pay the penny auction site for bids ahead of time, typically 50 cents to $1 dollar, usually in packs costing $25-$50. Once you have purchased the bids, you can use them to bid on items listed by the penny auction site (unlike traditional auctions, items are owned by the site, not third parties). Items typically start at or near $0 and each bid raises the price by a fixed amount, usually just a penny. Auctions are timed, and when the time runs out, the last and highest bidder wins the item. Although the price of the item itself may not be that high, the successful bidder will typically have spent much more than that. Unlike a traditional auction, it costs money to bid, and that money is gone even if the bidder does not win the auction. The bidder's cumulative cost of bidding must be added to the final price of a successful bid to determine the true cost of the item. The Federal Trade Commission has issued an alert about penny auctions, warning that bidders may find that they spend far more than they intended (Consumer Reports.org, 2013). Examples of penny auction sites include QuiBids, Beezid, and HappyBidDay.

WHEN TO USE AUCTIONS (AND FOR WHAT) IN BUSINESS

There are many different situations in which auctions are an appropriate channel for businesses to consider. For much of this chapter, we have looked at auctions from a consumer point of view. The objective of consumers is to receive the greatest value for the lowest cost. Now, switch your perspective to that of a business. Remember that the objective of businesses using auctions is to maximize their revenue (their share of consumer surplus) by finding the true market value of products and services, a market value that hopefully is higher in the auction channel than in fixed-price channels. **Table 11.6** provides an overview of factors to consider.

The factors are described as follows:

- **Type of product:** Online auctions are most commonly used for rare and unique products for which prices are difficult to discover, and there may have been no

the United States, the creator of intellectual property owns it. For instance, if you personally create an e-commerce site, it belongs entirely to you, and you have exclusive rights to use this "property" in any lawful way you see fit. But the Internet potentially changes things. Once intellectual works become digital, it becomes difficult to control access, use, distribution, and copying. These are precisely the areas that intellectual property seeks to control.

Digital media differ from books, periodicals, and other media in terms of ease of replication, transmission, and alteration; difficulty in classifying a software work as a program, book, or even music; compactness—making theft easy; and difficulty in establishing uniqueness. Before widespread use of the Internet, copies of software, books, magazine articles, or films had to be stored on physical media, such as paper, computer disks, or videotape, creating hurdles to distribution, and raising the costs of illegal copies.

The Internet technically permits millions of people to make perfect digital copies of various works—from music to plays, poems, and journal articles—and then to distribute them nearly cost-free to hundreds of millions of online users. The proliferation of innovation has occurred so rapidly that few entrepreneurs have stopped to consider who owns the patent on a business technique or method that they are using on their site. The spirit of the Web has been so free-wheeling that many entrepreneurs ignored trademark law and registered domain names that could easily be confused with another company's registered trademarks. In short, the Internet has demonstrated the potential to disrupt traditional conceptions and implementations of intellectual property law developed over the last two centuries.

The major ethical issue related to e-commerce and intellectual property concerns how we (both as individuals and as business professionals) should treat property that belongs to others. From a social point of view, the main questions are: Is there continued value in protecting intellectual property in the Internet age? In what ways is society better off, or worse off, for having the concept of property apply to intangible ideas, including music, books, and movies? Should society make certain technology illegal or restrict the use of the Internet just because it has an adverse impact on some intellectual property owners? From a political perspective, we need to ask how the Internet and e-commerce can be regulated or governed to protect the institution of intellectual property while at the same time encouraging the growth of e-commerce and the Internet.

TYPES OF INTELLECTUAL PROPERTY PROTECTION

There are three main types of intellectual property protection: copyright, patent, and trademark law. In the United States, the development of intellectual property law begins with the U.S. Constitution, which mandated Congress to devise a system of laws to promote "the progress of science and the useful arts." Congress passed the first copyright law in 1790 to protect original written works for a period of 14 years, with a 14-year renewal if the author was still alive. Since then, the idea of copyright has been extended to include music, films, translations, photographs, and most recently the designs of vessels under 200 feet (Fisher, 1999). The copyright law has been amended (mostly extended) 11 times in the last 40 years.

The goal of intellectual property law is to balance two competing interests—the public and the private. The public interest is served by the creation and distribution of inventions, works of art, music, literature, and other forms of intellectual expression. The private interest is served by rewarding people for creating these works through the creation of a time-limited monopoly granting exclusive use to the creator.

Maintaining this balance of interests is always challenged by the invention of new technologies. In general, the information technologies of the last century—from radio and television to CD-ROMs, DVDs, and the Internet—have at first tended to weaken the protections afforded by intellectual property law. Owners of intellectual property have often, but not always, been successful in pressuring Congress and the courts to strengthen the intellectual property laws to compensate for any technological threat, and even to extend protection for longer periods of time and to entirely new areas of expression. In the case of the Internet and e-commerce technologies, once again, intellectual property rights are severely challenged. In the next few sections, we discuss the significant developments in each area: copyright, patent, and trademark.

COPYRIGHT: THE PROBLEM OF PERFECT COPIES AND ENCRYPTION

copyright law protects original forms of expression such as writings, art, drawings, photographs, music, motion pictures, performances, and computer programs from being copied by others for a minimum of 70 years

In the United States, **copyright law** protects original forms of expression such as writings (books, periodicals, lecture notes), art, drawings, photographs, music, motion pictures, performances, and computer programs from being copied by others for a period of time. Up until 1998, the copyright law protected works of individuals for their lifetime plus 50 years beyond their life, and works created for hire and owned by corporations, such as Mickey Mouse of the Disney Corporation, for 75 years after initial creation. Copyright does not protect ideas—just their expression in a tangible medium such as paper, cassette tape, or handwritten notes.

In 1998, Congress extended the period of copyright protection for an additional 20 years, for a total of 95 years for corporate-owned works, and life plus 70 years of protection for works created by individuals (the Copyright Term Extension Act, also known as the CTEA). In *Eldred v. Ashcroft*, the Supreme Court ruled that the CTEA was constitutional, over the objections of groups arguing that Congress had given copyright holders a permanent monopoly over the expression of ideas, which ultimately would work to inhibit the flow of ideas and creation of new works by making existing works too expensive (*Eldred v. Ashcroft*, 2003; Greenhouse, 2003a). Librarians, academics, and others who depend on inexpensive access to copyrighted material opposed the legislation.

In the mid-1960s, the Copyright Office began registering software programs, and in 1980, Congress passed the Computer Software Copyright Act, which clearly provides protection for source and object code and for copies of the original sold in commerce, and sets forth the rights of the purchaser to use the software while the creator retains legal title. For instance, the HTML code for a web page—even though easily available to every browser—cannot be lawfully copied and used for a commercial purpose, say, to create a new website that looks identical.

Copyright protection is clear-cut: it protects against copying of 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 expression in a work. A competitor can view the source code on your website to see how various effects were created and then reuse those techniques to create a different website without infringing on your copyright.

Look and Feel

"Look and feel" copyright infringement lawsuits are precisely about the distinction between an idea and its expression. For instance, in 1988, Apple Computer sued Microsoft Corporation and Hewlett-Packard Inc. for infringing Apple's copyright on the Macintosh interface. Among other claims, Apple claimed that the defendants copied the expression of overlapping windows. Apple failed to patent the idea of overlapping windows when it invented this method of presenting information on a computer screen in the late 1960s. The defendants counterclaimed that the idea of overlapping windows could only be expressed in a single way and, therefore, was not protectable under the "merger" doctrine of copyright law. When ideas and their expression merge (i.e., if there is only one way to express an idea), the expression cannot be copyrighted, although the method of producing the expression might be patentable (*Apple Computer, Inc. v. Microsoft*, 1989). In general, courts appear to be following the reasoning of a 1992 case—*Brown Bag Software vs. Symantec Corp.*—in which the court dissected the elements of software alleged to be infringing. There, the Federal Circuit Court of Appeals found that neither similar concept, function, general functional features (e.g., drop-down menus), nor colors were protectable by copyright law (*Brown Bag vs. Symantec Corp.*, 1992).

Fair Use Doctrine

Copyrights, like all rights, are not absolute. There are situations where strict copyright observance could be harmful to society, potentially inhibiting other rights such as the right to freedom of expression and thought. As a result, the doctrine of fair use has been created. The **doctrine of fair use** permits teachers, writers, and others to use copyrighted materials without permission under certain circumstances. **Table 8.12** describes the five factors that courts consider when assessing what constitutes fair use.

doctrine of fair use under certain circumstances, permits use of copyrighted material without permission

The fair use doctrine draws upon the First Amendment's protection of freedom of speech (and writing). Journalists, writers, and academics must be able to refer to, and cite from, copyrighted works in order to criticize, or even discuss them. Professors are allowed to clip a contemporary article just before class, copy it, and hand it out to students as an example of a topic under discussion. However, they are not permitted to add this article to the class syllabus for the next semester without compensating the copyright holder.

What constitutes fair use has been at issue in a number of recent cases. In *Kelly v. Arriba Soft* (2003) and *Perfect 10, Inc. v. Amazon.com, Inc. et al.,* (2007), the Federal Circuit Court of Appeals for the 9th Circuit held that the display of thumbnail images in response to search requests constituted fair use. A similar result was reached by the district court for the District of Nevada with respect to Google's storage and display of websites from cache memory, in *Field v. Google, Inc.* (2006). In all of these cases, the courts accepted the argument that caching the material and displaying it in response

TABLE 8.12 FAIR USE CONSIDERATIONS TO COPYRIGHT PROTECTIONS

FAIR USE FACTOR	INTERPRETATION
Character of use	Nonprofit or educational use versus for-profit use.
Nature of the work	Creative works such as plays or novels receive greater protection than factual accounts, e.g., newspaper accounts.
Amount of work used	A stanza from a poem or a single page from a book would be allowed, but not the entire poem or a book chapter.
Market effect of use	Will the use harm the marketability of the original product? Has it already harmed the product in the marketplace?
Context of use	A last-minute, unplanned use in a classroom versus a planned infringement.

to a search request was not only a public benefit, but also a form of marketing of the material on behalf of its copyright owner, thereby enhancing the material's commercial value. In what's known as the "dancing baby case," a mother uploaded a 30-second video to YouTube of her baby dancing to a song by Prince called Let's Go Crazy. Universal Music Group, the owner of the copyright to the song, objected and issued a DMCA takedown notice to YouTube. The mother sued, claiming that Universal failed to consider whether use of the song in the video was fair use before issuing the takedown notice. The 9th Circuit Court of Appeals agreed that a copyright owner must consider fair use before sending a takedown notice. The ruling has been appealed to the Supreme Court (Morran, 2016; Bergen, 2015).

Fair use was also at issue in a lawsuit filed by the Authors Guild and five major publishing companies against Google. In 2004, Google announced a book project with two parts. A Partner Program would scan books with the permission of publishers, index the books, post snippets of the books on line, and make bibliographic information available on Google's search engine. In the second project, called the Library Project, Google aimed to scan all the books in several university and public libraries, and then make snippets and parts of the book available online without receiving permission from the publishers or paying royalties. Google said it would never show a full page, just relevant portions of a page in response to searches. In 2005, the Authors Guild and the large book publishers filed a lawsuit seeking to prevent Google from implementing the Library Project.

Google argued that the Library Project constituted fair use of publishers' copyrighted works because it only published snippets. Moreover, Google claimed that it was simply helping libraries do what they are intended to do, namely, lend books. Library lending is considered a fair use following an agreement in the late 1930s with publishers, and such lending was codified into the Copyright Act of 1976. Google claimed that helping libraries make books more available to the public was in the broader public interest, and extended existing rights of libraries to encourage book availability.

In 2013, eight years later, a federal court finally found in favor of Google without reservation by ruling that Google's scanning and making snippets of text available to the public was "fair use" under U.S. copyright law. The judge believed the project had a broad public purpose of making it easier for students, researchers, teachers, and the general public to find books, while also preserving consideration for author and publisher rights. The Google project was "transformative" in the court's view, giving books a new character and purpose, making it easier to discover old books, and leading to increased sales. After a decade of litigation, the Supreme Court ruled in 2016 that Google's Library Project was fair use, and the matter is settled from a legal perspective (Liptak and Alter, 2016). In the meantime, the project itself has stalled, and efforts to scan so-called orphan books in libraries where the copyright holder could not be identified have ended. Google now appears less than enthusiastic about pursuing the project, in part, analysts believe, because the project offered no hope of ever making a return on the investment, and created a rift with the author and publishing community.

The Digital Millennium Copyright Act of 1998

Digital Millennium Copyright Act (DMCA)
the first major effort to adjust the copyright laws to the Internet age

The **Digital Millennium Copyright Act (DMCA)** of 1998 was the first major effort to adjust the copyright laws of the United States to the Internet age, and remains to this day, the primary statute that defines the relationship between copyright owners, Internet service providers (which in this context also includes website publishers as well as firms that provide Internet service), and end-users of copyrighted material. The law implements two international treaties of the World Intellectual Property Organization (WIPO), a worldwide body formed by the major nations in North America and Europe, as well as Japan. This is one case where law preceded or at least was contemporaneous with digital technology. **Table 8.13** summarizes the major provisions of the DMCA.

There are a number of different actors and conflicting interests involved in the process of delivering content on the Internet. Obviously, copyright owners do not want their work copied and distributed without their consent (and probably compensation), and they do not want their digital rights management software programs broken, compromised, or made ineffectual. ISPs want the freedom to use content within the provisions of "fair use" and do not want to be held liable for content that users may post to their websites. ISPs argue that they are similar to telephone transmission lines, merely providing a method of communication, and they should not be required to monitor their users' activities to see if they are posting copyrighted material. Such surveillance, ISPs and civil libertarians argue, would constitute a restriction on freedom of expression. In addition, the economics of the Internet could be compromised if ISPs were unnecessarily restricted and pay the costs of vetting all content posted by users. The business model of many Internet firms depends on creating large, even huge, audiences, and the more content that can be displayed, the larger the audience, and the more ads can be sold. ISPs also generate revenue from selling bandwidth, so the greater the bandwidth required to support large audiences, the better it is for them. Restricting content is bad for business. Finally, consumers of Internet content want as much content as possible, at the lowest cost possible, or even free. The more content for users to consume, the more they benefit from the Internet.

TABLE 8.13 THE DIGITAL MILLENNIUM COPYRIGHT ACT

SECTION	IMPORTANCE
Title I, WIPO Copyright and Performances and Phonograms Treaties Implementation	Makes it illegal to circumvent technological measures to protect works for either access or copying or to circumvent any electronic rights management information.
Title II, Online Copyright Infringement Liability Limitation	Limits liability of ISPs and search engines for copyright infringement if they comply with safe harbors. Requires ISPs to "take down" sites they host if they are infringing copyrights, and requires search engines to block access to infringing sites if they receive proper notice of infringement from the copyright owner.
Title III, Computer Maintenance Competition Assurance	Permits users to make a copy of a computer program for maintenance or repair of the computer.
Title IV, Miscellaneous Provisions	Requires the Copyright Office to report to Congress on the use of copyright materials for distance education; allows libraries to make digital copies of works for internal use only; extends musical copyrights to include "webcasting."

SOURCE: Based on data from United States Copyright Office, 1998.

The DMCA tries to balance these different interests. Title I of the DMCA implements the WIPO Copyright Treaty of 1996, which makes it illegal to make, distribute, or use devices that circumvent technology-based protections of copyrighted materials, and attaches stiff fines and prison sentences for violations. This makes it illegal, for instance, to break the security software typically found on DVDs, Amazon's Kindle books, and similar devices. There are a number of exceptions to the strong prohibitions against defeating a copyright protection scheme, however, including exceptions for libraries to examine works for adoption, for reverse engineering to achieve interoperability with other software, for encryption research, and for privacy protection purposes.

Title II of the DMCA creates two safe harbors for ISPs. The first safe harbor (the Online Copyright Infringement Liability Limitation Act) provides that ISPs will not be held liable for infringing material that users post to blogs, web pages, or forums, as long as the ISP did not have knowledge that the content was infringing, did not receive any financial benefit attributable to the infringing activity (assuming they can control this activity), and acts expeditiously to remove infringing content when notified by a notice of infringement. This means that users of, say, YouTube, can post material that infringes a copyright and YouTube cannot be held liable (safe harbor) as long as it does not know the material is infringing, and if it demonstrates that it has in place procedures to take down infringing content once it becomes aware of the matter or receives a proper notice from the copyright owner. Such a notice is called a takedown

notice, a claim by the copyright owner that the ISP is hosting infringing content. Copyright owners can also subpoena the personal identities of any infringers using an ISP.

The second safe harbor relates to links to infringing material: ISPs will not be held liable for referring or linking users to a site that contains infringing material or infringing activity. So for example, a search engine that directs users to a website that contains pirated songs or movies cannot be held liable. This safe harbor is applicable as long as ISPs did not have knowledge they were linking users to sites containing infringing content, did not receive any financial benefit attributable to the infringing activity (assuming they can control this activity), and acts expeditiously to remove or disable any such link after receiving a proper notice from the copyright owner.

There are a number of administrative requirements for ISPs to be protected by the safe harbor provisions. ISPs must designate an agent to receive takedown notices; adopt and publish a copyright infringement policy (this can be part of a terms of use policy); and comply with takedown notices by removing the content, and/or links to the content. The penalties for willfully violating the DMCA include restitution to the injured parties of any losses due to infringement. Criminal remedies may include fines up to $500,000 or five years imprisonment for a first offense, and up to $1 million in fines and 10 years in prison for repeat offenders. These are serious penalties, but they have rarely been imposed.

The DMCA relieves ISPs of any liability for posting or linking to copyrighted material, if they can meet the safe harbors' conditions. This means users of YouTube can post what they want, and YouTube will not be held liable for infringing content even if it violates YouTube's terms of use policy, which states that users shall not post infringing content. However, it does require YouTube to remove content or links that are infringing once it receives a valid takedown notice. With respect to receiving financial benefits, ISPs may indeed receive financial benefits from posting infringing content if they can show that they can't control the behavior of their users, or that there is no way of knowing prior to the posting that the material is infringing. For instance, how can YouTube be held responsible for users who post copyrighted songs or movies? How could YouTube know, at the time of posting, that the content is infringing?

ISPs and individuals who post content are also protected from frivolous takedown notices. For instance, the ruling in the "dancing baby" case discussed on page 535 put copyright owners on notice that they needed to be careful issuing takedown notices if use of the copyrighted material might constitute fair use and that the DMCA does not supersede the doctrine of fair use.

Safe harbor provisions of the DMCA were also at the heart of a $1 billion lawsuit originally brought by Viacom in 2007 against Google and YouTube for willful copyright infringement. In the Viacom case, Viacom alleged that YouTube and Google engaged in massive copyright infringement by deliberately and knowingly building up a library of infringing works to draw traffic to the YouTube site and enhance its commercial value. Entire episodes of shows like SpongeBob SquarePants and The Daily Show were appearing on YouTube without permission or payment. In response, Google and YouTube claimed that they are protected by the DMCA's safe harbor provisions and that it is impossible to know whether a video is infringing or not. YouTube also does

not display ads on pages where consumers can view videos unless it has an agreement with the content owner. In 2007, Google announced a filtering system (Content ID) aimed at addressing the problem. It requires content owners to give Google a copy of their content so Google can load it into an auto-identification system. Then after a video is uploaded to YouTube, the system attempts to match it with its database of copyrighted material and removes any unauthorized material. The copyright owner has several options: it can mute the audio; block a whole video; monetize the video by running ads against it; and track the video's viewer statistics. In 2014, seven years after the billion dollar suit was filed, and multiple court room appearances, Google and Viacom settled out of court. Google's ability to take down copyrighted material using Content ID had become very effective, and Google agreed to rent hundreds of Viacom shows (Kaufman, 2014). Both parties recognized in a joint statement that they could achieve their objectives by collaborating rather than continuing the lawsuit.

The entertainment industry continues to be aggressive in pursuing online copyright infringement. In 2012, the U.S. Department of Justice seized the domain Megaupload.com, one of the largest cyberlockers on the Internet dedicated to storing and sharing copyrighted movies and music. A **cyberlocker** is an online file storage service dedicated to sharing copyrighted material (often movies) illegally. Megaupload's founder, Kim Dotcom, was arrested in New Zealand at his home, and $17 million in assets, and later, $37 million in cash in Hong Kong, was confiscated. Mr. Dotcom is currently back in court, and fighting efforts by the United States to extradite him from New Zealand to face copyright, racketeering, and money laundering charges (Reuters, 2015). In 2016, the U.S. federal government seized Mr. Dotcom's assets that were located in the United States, along with the assets of others associated with him, pending his extradition to the United States to face criminal piracy charges.

cyberlocker
an online file storage service dedicated to sharing copyrighted material illegally

Since the Megaupload case, other cyberlockers have restricted their activities to avoid a similar fate as Megaupload. In 2013, the Center for Copyright Information (CCI), along with 5 of the largest ISPs, major entertainment industry companies, and the Consumer Advisory Board launched the Copyright Alert System (CAS)—a tiered notice and response system aimed at reducing copyright infringement over P2P networks. During its first 10 months of operation, the CAS sent out over 1.3 million alerts to 720,000 ISP account holders of alleged copyright infringement. If the account holder ignores repeated alerts, their ISP may impose consequences, such as a downgrade of the customer's Internet service. The CCI believes that the CAS has great promise for its ability to move user behavior away from copyright infringement and toward legal sources of content (Center for Copyright Information, 2014). Refer to the chapter-ending case study on The Pirate Bay.

In 2016, DMCA litigation continues. In *BMG Rights Management v. Cox Communications*, a federal judge let stand a $25 million jury award against Cox Cable in favor of BMG, a rights management firm, for willful contributory infringement. BMG argued that Cox, an ISP, was allowing subscribers to use BitTorrent to upload copyrighted songs to various websites without an effective policy for preventing this activity, and failing to remove repeat offenders from its service. Cox argued that it was just a pipeline to the Internet and could not be held liable for what its users posted or what software they

used. However, although the court left the jury award against Cox in place, it refused to enjoin Cox from continuing to operate, as BMG had requested, noting that while there is a public benefit to reducing copyright infringement, because Cox provides access to the Internet and enables freedom of speech, these interests trumped BMG's interest in copyright protection (Gardner, 2016).

Also in 2016, a federal court ruled that the video sharing site Vimeo was protected by DMCA against liability for allowing users to post copyrighted video and music created prior to 1972 when DMCA became law. Vimeo did have a procedure of accepting infringement notices and taking down infringing content, but some pre-1972 music tracks were still on the site despite repeated takedown notices (*Capital Records v. Vimeo LLC*, 2016).

Copyright owners from the film and music industry are lobbying Congress for changes in the DMCA that would require websites and ISPs to take more effective actions in removing infringing content (Raymond, 2016). Musicians and film makers have begun to protest the compensation they receive from streaming services (see Chapter 10).

While there has been some progress in limiting infringing content on the Internet, new mobile apps such as Periscope and Meerkat make it easy for people to capture live video and stream it to these apps on mobile devices, making it extremely difficult for content owners to protect the value of their live products. Periscope is owned by Twitter and users can post live videos to Twitter. Meerkat can post live video streams to most social network sites, including Facebook. In 2015, Periscope and Meerkat were used by thousands of users to watch the pay-per-view broadcast of the welterweight fight between Floyd Mayweather and Manny Pacquiao for free. The pay-per-view price on cable networks was $100. Other users have streamed live TV series such as HBO's Game of Thrones. Periscope received 1,400 DMCA takedown requests in the first three months of its existence. Twitter says it has complied with 71% of these (Weber, 2015). But the DMCA takedown notices do not help a unique live event such as a championship boxing match retain its value. The value of the event is largely in attracting viewers willing to pay to see it as it happens, and once a free alternative is available, that value is diminished.

PATENTS: BUSINESS METHODS AND PROCESSES

> **"Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title."**
>
> —Section 101, U.S. Patent Act

patent
grants the owner an exclusive monopoly on the ideas behind an invention for 20 years

A **patent** grants the owner a 20-year exclusive monopoly on the ideas behind an invention. The congressional intent behind patent law was to ensure that inventors of new machines, devices, or industrial methods would receive the full financial and other rewards of their labor and still make widespread use of the invention possible by

providing detailed diagrams for those wishing to use the idea under license from the patent's owner. Patents are obtained from the United States Patent and Trademark Office (USPTO), which was created in 1812. Obtaining a patent is much more difficult and time-consuming than obtaining copyright protection (which is automatic with the creation of the work). Patents must be formally applied for, and the granting of a patent is determined by Patent Office examiners who follow a set of rigorous rules. Ultimately, federal courts decide when patents are valid and when infringement occurs.

Patents are very different from copyrights because patents protect the ideas themselves and not merely the expression of ideas. There are four types of inventions for which patents are granted under patent law: machines, man-made products, compositions of matter, and processing methods. The Supreme Court has determined that patents extend to "anything under the sun that is made by man" (*Diamond v. Chakrabarty*, 1980) as long as the other requirements of the Patent Act are met. There are three things that cannot be patented: laws of nature, natural phenomena, and abstract ideas. For instance, a mathematical algorithm cannot be patented unless it is realized in a tangible machine or process that has a "useful" result (the mathematical algorithm exception).

In order to be granted a patent, the applicant must show that the invention is new, original, novel, nonobvious, and not evident in prior arts and practice. As with copyrights, the granting of patents has moved far beyond the original intent of Congress's first patent statute, which sought to protect industrial designs and machines. Patent protection has been extended to articles of manufacture (1842), plants (1930), surgical and medical procedures (1950), and software (1981). The Patent Office did not accept applications for software patents until a 1981 Supreme Court decision that held that computer programs could be a part of a patentable process. Since that time, thousands of software patents have been granted. Virtually any software program can be patented as long as it is novel and not obvious.

Essentially, as technology and industrial arts progress, patents have been extended to both encourage entrepreneurs to invent useful devices and promote widespread dissemination of the new techniques through licensing and artful imitation of the published patents (the creation of devices that provide the same functionality as the invention but use different methods) (Winston, 1998). Patents encourage inventors to come up with unique ways of achieving the same functionality as existing patents. For instance, Amazon's patent on one-click purchasing caused Barnesandnoble.com to invent a simplified two-click method of purchasing.

The danger of patents is that they stifle competition by raising barriers to entry into an industry. Patents force new entrants to pay licensing fees to incumbents, and thus slow down the development of technical applications of new ideas by creating lengthy licensing applications and delays. Nowhere is the tradeoff between encouraging innovation and yet avoiding raising barriers to market entry (and thereby discouraging innovation) more evident than in the patent battle that has raged between Apple and Samsung in the smartphone market.

In 2011, Apple filed suit in the United States against Samsung alleging that Samsung's Galaxy smartphones violated Apple patents on its iPhone and iPad computer. By 2012, Apple and Samsung were involved in over 50 different patent lawsuits through-

TABLE 8.14 APPLE/SAMSUNG SMARTPHONE PATENT WARS

YEAR	DESCRIPTION
2011–2012	In 2011 Apple filed suit in the United States charging Samsung devices violated Apple patents, and Samsung claimed similar infringement by Apple. The smartphone patent wars begin. Apple's patents had been filed in January 2007 shortly after the introduction of the iPhone. The design patents covered the basic shape of the phone, software features (slide-to-unlock, autocorrect, bounce-back effect, and quicklinks), trade dress features, and user interface (home button and icons with rounded and tapered edges). In short, everything that made the iPhone a unique product. By 2012, Apple and Samsung are involved in 50 different lawsuits around the world involving the design of tablets and smartphones.
August 2012	First jury verdict mostly favorable to Apple. Found Samsung had infringed on design and utility patents, and Apple's trade dress features. Awarded Apple $1.049 billion. An injunction preventing Samsung from selling infringing products was at first denied, but later granted.
November 2013	A retrial of the first jury trial. Samsung admitted to infringing on Apple patents, but argued the penalty was too high. The jury reduced the damages to $290 million.
May 2014	Another jury trial. Apple wins jury verdict of $119.6 million against Samsung, finding that Samsung infringed on patents for slide-to-unlock, autocorrect, and quicklinks features. Judge declines to force removal of devices from market, instead argues for damages as penalty.
September 2015	Apple and Samsung announced an agreement to participate in court-supervised mediation of their five-year dispute. This is the third effort at mediation (the first two failed).
2016	Apple asks the Supreme Court to rule that Samsung must pay $548 million to Apple for patent infringment based on the value of the entire phone, not just its specific design elements which Samsung argues are a small part of the phone's value.

out the world. See **Table 8.14** for a brief history of the Apple/Samsung smartphone patent wars.

The history of the patent battle is quite complex, and lengthy, lasting over five years. There are three questions raised in this litigation. First, does Apple have valid patents on iPhone and iPad hardware and software? Second, did Samsung's phones and tablets infringe on these Apple patents? And third, if Samsung did infringe, what should the penalty be? There are two possibilities: Samsung pays a fine for damages and/or Samsung removes its infringing products from the market. A fourth question is separate from the lawsuits per se and concerns society, the rest of us: what is the best outcome for society?

After five years and two jury trials, the courts have decided that Apple does have valid patents on the physical iPhone, as well as the operating system, including the physical design (rounded corners and bezel), user interface, and screen functionality. Second, the courts did find that Samsung infringed on some of Apple's patents,

and even Samsung admits as much. Third, the courts have generally avoided forcing Samsung to remove its infringing devices from the market, and instead have focused on damages with some exceptions for older phones (Decker, 2015). However, in September 2015, Apple finally won a U.S. appeals court judgment that enjoins Samsung from selling smartphones with Apple's patented slide-to-unlock, autocorrect, and quicklinks features. This was a major victory in principle that Apple can use in the future against other copycat firms (Chen, 2015; Kendall and Wakabayashi, 2015). But Samsung had already designed around these features and came up with its own user interface that accomplishes the same tasks. Hence, the ruling is not likely to have a notable impact on Samsung's sales revenues. The original jury award of $1 billion has been whittled down over the years. Analysts believe the cost to Apple of this litigation is at least equal to the damage award it may ultimately be paid. Over the last five years of litigation, Samsung has changed its interface and functionality to greatly reduce its infringement. Software features can always be designed around. In 2016, Apple asked the Supreme Court to rule that Samsung must pay for its patent infringement based on all of the profits it made on the entire phone. Samsung argued it should only be liable for that portion of the profits attributable to the design of the phones, a much smaller liability (Kendall, 2016). The final chapter may not be closed until 2017.

An answer to the fourth question, what is the best outcome for society, is more difficult to determine. Apple's forceful defense has put copycat firms on notice that if they infringe on patents owned by large firms such as Apple, it could be harmful to their brands and possibly result in significant damages. Samsung has been pushed into the lower end of the market where it competes with less expensive, copycat smartphones from China. Samsung has a very large chunk of the smartphone market worldwide, but it has been denied pricing power and resulting profits. The litigation may have strengthened Apple's claim that its computers and smartphones are truly unique, and original. Apple today is the largest corporation in the United States by market capitalization and also the most profitable in the world. Samsung's copying of Apple designs and features may only have strengthened Apple's claims to be a superior product.

E-commerce Patents

Much of the Internet's infrastructure and software was developed under the auspices of publicly funded scientific and military programs in the United States and Europe. Unlike Samuel F. B. Morse, who patented the idea of Morse code and made the telegraph useful, most of the inventions that make the Internet and e-commerce possible were not patented by their inventors. The early Internet was characterized by a spirit of worldwide community development and sharing of ideas without consideration of personal wealth (Winston, 1998). This early Internet spirit changed in the mid-1990s with the commercial development of the Web.

In 1998, a landmark legal decision, *State Street Bank & Trust v. Signature Financial Group, Inc.*, paved the way for business firms to begin applying for "business methods" patents. In this case, a Federal Circuit Court of Appeals upheld the claims of Signature Financial to a valid patent for a business method that allows managers to monitor and record financial information flows generated by a partner fund. Previously, it was

thought business methods could not be patented. However, the court ruled there was no reason to disallow business methods from patent protection, or any "step by step process, be it electronic or chemical or mechanical, [that] involves an algorithm in the broad sense of the term" (*State Street Bank & Trust Co. v. Signature Financial Group*, 1998). The State Street decision led to an explosion in applications for e-commerce "business methods" patents. In 2010, the U.S. Supreme Court issued a divided opinion on business methods patents in the *Bilski et al. v. Kappos* case (*Bilski et al. v. Kappos*, 2010). The majority argued that business methods patents were allowable even though they did not meet the traditional "machine or transformation test," in which patents are granted to devices that are tied to a particular machine, are a machine, or transform articles from one state to another. The minority wanted to flatly declare that business methods are not patentable in part because any series of steps could be considered a business method (Schwartz, 2010). The Supreme Court struck another blow against business method patents in 2014, with its decision in *Alice Corporation vs. CLS Bank International*. The Court ruled that basic business methods cannot be patented and that while software can be patented, implementing an abstract idea that otherwise could not be patented by using software does not transform the idea into a patentable innovation (*Alice Corporation Pty. Ltd. v. CLS Bank International*, 2014).

Table 8.15 lists some of the better-known e-commerce patents. Some are controversial. Reviewing these, you can understand the concerns of commentators and corporations. Some of the patent claims are very broad (for example, "name your price" sales methods), have historical precedents in the pre-Internet era (shopping carts), and seem "obvious" (one-click purchasing). Critics of online business methods patents argue that the Patent Office has been too lenient in granting such patents, and that in most instances, the supposed inventions merely copy pre-Internet business methods and thus do not constitute "inventions" (Harmon, 2003; Thurm, 2000; Chiappetta, 2001). The Patent Office argues, on the contrary, that its Internet inventions staff is composed of engineers, lawyers, and specialists with many years of experience with Internet and network technologies, and that it consults with outside technology experts before granting patents. To complicate matters, the European Patent Convention and the patent laws of most European countries do not recognize business methods per se unless the method is implemented through some technology (Takenaka, 2001).

TRADEMARKS: ONLINE INFRINGEMENT AND DILUTION

> A trademark is "any word, name, symbol, or device, or any combination thereof ... used in commerce ... to identify and distinguish ... goods ... from those manufactured or sold by others and to indicate the source of the goods."
>
> —The Trademark Act, 1946

trademark
a mark used to identify and distinguish goods and indicate their source

Trademark law is a form of intellectual property protection for **trademarks**—a mark used to identify and distinguish goods and indicate their source. Trademark protections exist at both the federal and state levels in the United States. The purpose of trademark

TABLE 8.15 SELECTED E-COMMERCE PATENTS

COMPANY	SUBJECT	UPDATE
Amazon	One-click purchasing	Amazon attempted to use patent originally granted to it in 1999 to force changes to Barnes & Noble's website, but a federal court overturned a previously issued injunction. Eventually settled out of court. In 2007, a USPTO panel rejected some of the patent because of evidence another patent predated it. Amazon amended the patent, and the revised version was confirmed in 2010.
Priceline	Buyer-driven "name your price" sales	Originally filed by Walker Digital, an intellectual property laboratory, and then assigned to Priceline. Granted by the USPTO in 1999. Shortly thereafter, Priceline sued Microsoft and Expedia for copying its patented business method.
Akamai	Internet content delivery global hosting system	A broad patent granted in 2000 covering techniques for expediting the flow of information over the Internet. Akamai sued Digital Island for violating the patent and, in 2001, a jury found in its favor.
DoubleClick	Dynamic delivery of online advertising	The patent underlying DoubleClick's business of online banner ad delivery, originally granted in 2000. DoubleClick sued competitors 24/7 Media and L90 for violating the patent and ultimately reached a settlement with them.
Overture	Pay for performance search	System and method for influencing position on search result list generated by computer search engine, granted in 2001. Competitor FindWhat sued Overture, charging that patent was obtained illegally; Overture countered by suing both FindWhat and Google for violating patent. Google agreed to pay a license fee to Overture in 2004 to settle.
Acacia Technologies	Streaming video media transmission	Patents for the receipt and transmission of streaming digital audio and/or video content originally granted to founders of Greenwich Information Technologies in 1990s. Patents were purchased by Acacia, a firm founded solely to enforce the patents, in 2001.
Soverain Software	Purchase technology	The so-called "shopping cart" patent for network-based systems, which involves any transaction over a network involving a seller, buyer, and payment system. In other words, e-commerce! Soverain filed suit against Amazon for patent infringement, which Amazon paid $40 million to settle. In 2013 a federal district court ruled Soverain's claims against Newegg in part invalid.
MercExchange (Thomas Woolston)	Auction technology	Patents on person-to-person auctions and database search, originally granted in 1995. eBay ordered to pay $25 million in 2003 for infringing on patent. In 2007, a motion for permanent patent injunction against eBay was denied. MercExchange and eBay settled the dispute in 2008 on confidential terms.
Google	Search technology	Google PageRank patent filed in 1998 and granted in 2001. Became non-exclusive in 2011 and expires in 2017.
Google	Location technology	Patent for a method of using location information in an advertising system issued to Google in 2010.
Apple	Social technology	Apple applied for a patent in 2010 that allows groups of friends attending events to stay in communication with each other and share reactions to live events as they are occurring.
Facebook	Social technology	A 2010 patent on an algorithm for developing personalized stories and newsfeeds on a social network.

law is twofold. First, trademark law protects the public in the marketplace by ensuring that it gets what it pays for and wants to receive. Second, trademark law protects the owner—who has spent time, money, and energy bringing the product to the marketplace—against piracy and misappropriation. Trademarks have been extended from single words to pictures, shapes, packaging, and colors. Some things may not be trademarked such as common words that are merely descriptive ("clock"). Federal trademarks are obtained, first, by use in interstate commerce, and second, by registration with the U.S. Patent and Trademark Office (USPTO). Federal trademarks are granted for a period of 10 years and can be renewed indefinitely.

Disputes over federal trademarks involve establishing infringement. The test for infringement is twofold: market confusion and bad faith. Use of a trademark that creates confusion with existing trademarks, causes consumers to make market mistakes, or misrepresents the origins of goods is an infringement. For instance, in 2015, Multi Time Machine (MTM) sued Amazon for violation of its trademarks and confusing consumers looking to buy MTM watches. MTM makes military style watches that are not sold on Amazon. If a user searches on Amazon for an MTM watch, the search results shows watches being offered by MTM competitors that are similar in style to MTM's. MTM argued that this could confuse customers and the court agreed, allowing the case to proceed to trial (Levine, 2015). In addition, the intentional misuse of words and symbols in the marketplace to extort revenue from legitimate trademark owners ("bad faith") is proscribed.

In 1995, Congress passed the Federal Trademark Dilution Act (FTDA), which created a federal cause of action for dilution of famous marks. This legislation dispenses with the test of market confusion (although that is still required to claim infringement), and extends protection to owners of famous trademarks against **dilution**, which is defined as any behavior that would weaken the connection between the trademark and the product. In 2006, the FTDA was amended by the Trademark Dilution Revision Act (TDRA), which allows a trademark owner to file a claim based on a "likelihood of dilution" standard, rather than having to provide evidence of actual dilution. The TDRA also expressly provides that dilution may occur through blurring (weakening the connection between the trademark and the goods) and tarnishment (using the trademark in a way that makes the underlying products appear unsavory or unwholesome). Internationally, WIPO handles many cybersquatting cases under its Uniform Dispute Resolution Procedures. In 2014, WIPO warned that the expansion of generic top-level domains authorized by ICANN is likely to be very disruptive in terms of trademark protection (New, 2014). Although the cost of obtaining a new gTLD is not unsubstantial (it is estimated to be more than $180,000), by May 2015, 583 new gTLDs had been approved. Successful applicants become owners of these gTLDs, and can create and sell new domains with the gTLD suffix, such as Avenger.movie. Many of these new domains may potentially conflict with the established trademarks of others.

dilution
any behavior that would weaken the connection between the trademark and the product

To deal with these trademark conflicts, ICANN developed a set of procedures to rapidly resolve disputes called the Uniform Rapid Suspension System (URS), a domain name dispute procedure that allows a trademark owner to seek suspen-

sion of a domain name in a new generic top-level domain (gTLD). ICANN also established a Trademark Clearing house as a repository of data on registered, court-validated, or statute-protected trademarks. Trademark owners register their marks for a fee.

One successful applicant for a new gTLD is Vox Populi Registry Ltd. Based in the U.K., Vox purchased the gTLD .sucks, and began selling domains such as Apple.sucks and CitiGroup.sucks exclusively to corporations who did not want their brand name associated with .sucks. At some point, .sucks domains will be available to the general public, at which point anyone would be able to create a new domain that potentially embarrasses a major brand name or casts it in a negative light (Bloomberg News, 2015). ICANN has said it may seek remedies and has alerted the FTC and asked for an opinion on the legality of Vox Populi's behavior. ICANN is not a regulatory agency with enforcement powers, and its agreement with new domain owners does not discuss their business models (Fung, 2015).

Trademarks and the Internet

The rapid growth and commercialization of the Internet have provided unusual opportunities for existing firms with distinctive and famous trademarks to extend their brands to the Internet. These same developments have provided malicious individuals and firms the opportunity to squat on Internet domain names built upon famous marks, as well as attempt to confuse consumers and dilute famous or distinctive marks (including your personal name or a movie star's name). The conflict between legitimate trademark owners and malicious firms was allowed to fester and grow because Network Solutions Inc. (NSI), originally the Internet's sole agency for domain name registration for many years, had a policy of "first come, first served." This meant anyone could register any domain name that had not already been registered, regardless of the trademark status of the domain name. NSI was not authorized to decide trademark issues (Nash, 1997).

In response to a growing number of complaints from owners of famous trademarks who found their trademark names being appropriated by web entrepreneurs, Congress passed the **Anticybersquatting Consumer Protection Act (ACPA)** in 1999. The ACPA creates civil liabilities for anyone who attempts in bad faith to profit from an existing famous or distinctive trademark by registering an Internet domain name that is identical or confusingly similar to, or "dilutive" of, that trademark. The act does not establish criminal sanctions. It proscribes using "bad-faith" domain names to extort money from the owners of the existing trademark **(cybersquatting)**, or using the bad-faith domain to divert web traffic to the bad-faith domain that could harm the good will represented by the trademark, create market confusion, or tarnish or disparage the mark **(cyberpiracy)**. It is conceivable that domains such as the previously described Apple.sucks might be seen as a kind of cybersquatting and a violation of the ACPA. The act also proscribes the use of a domain name that consists of the name of a living person, or a name confusingly similar to an existing personal name, without that person's consent, if the registrant is registering the name with the intent to profit by selling the domain name to that person.

Anticybersquatting Consumer Protection Act (ACPA)
creates civil liabilities for anyone who attempts in bad faith to profit from an existing famous or distinctive trademark by registering an Internet domain name that is identical or confusingly similar to, or "dilutive" of, that trademark

cybersquatting
involves the registration of an infringing domain name, or other Internet use of an existing trademark, for the purpose of extorting payments from the legitimate owners

cyberpiracy
involves the same behavior as cybersquatting, but with the intent of diverting traffic from the legitimate site to an infringing site

TABLE 8.16 INTERNET AND TRADEMARK LAW EXAMPLES

ACTIVITY	DESCRIPTION	EXAMPLE CASE
Cybersquatting	Registering domain names similar or identical to trademarks of others to extort profits from legitimate holders	*E. & J. Gallo Winery v. Spider Webs Ltd.*, 129 F. Supp. 2d 1033 (S.D. Tex., 2001) aff'd 286 F. 3d 270 (5th Cir., 2002)
Cyberpiracy	Registering domain names similar or identical to trademarks of others to divert web traffic to their own sites	*Ford Motor Co. v. Lapertosa*, 2001 U.S. Dist. LEXIS 253 (E.D. Mich., 2001); *PaineWebber Inc. v. Fortuny*, Civ. A. No. 99-0456-A (E.D. Va., 1999); *Playboy Enterprises, Inc. v. Global Site Designs, Inc.*, 1999 WL 311707 (S.D. Fla., 1999); *Audi AG and Volkswagen of America Inc. v. Bob D'Amato* (No. 05-2359; 6th Cir., November 27, 2006)
Metatagging	Using trademarked words in a site's metatags	*Bernina of America, Inc. v. Fashion Fabrics Int'l, Inc.*, 2001 U.S. Dist. LEXIS 1211 (N.D. Ill., 2001); *Nissan Motor Co., Ltd. v. Nissan Computer Corp.*, 289 F. Supp. 2d 1154 (C.D. Cal., 2000), aff'd, 246 F. 3rd 675 (9th Cir., 2000)
Keywording	Placing trademarked keywords on web pages, either visible or invisible	*Playboy Enterprises, Inc. v. Netscape Communications, Inc.*, 354 F. 3rd 1020 (9th Cir., 2004); *Nettis Environment Ltd. v. IWI, Inc.*, 46 F. Supp. 2d 722 (N.D. Ohio, 1999); *Government Employees Insurance Company v. Google, Inc.*, Civ. Action No. 1:04cv507 (E.D. VA, 2004); *Google, Inc. v. American Blind & Wallpaper Factory, Inc.*, Case No. 03-5340 JF (RS) (N.D. Cal., April 18, 2007)
Linking	Linking to content pages on other sites, bypassing the home page	*Ticketmaster Corp. v. Tickets.com*, 2000 U.S. Dist. Lexis 4553 (C.D. Cal., 2000)
Framing	Placing the content of other sites in a frame on the infringer's site	*The Washington Post, et al. v. TotalNews, Inc., et al.*, (S.D.N.Y., Civil Action Number 97-1190)

Trademark abuse can take many forms on the Web. **Table 8.16** lists the major behaviors on the Internet that have run afoul of trademark law and some of the court cases that resulted.

Cybersquatting and Brandjacking

In one of the first cases involving the ACPA, E. & J. Gallo Winery, owner of the registered mark "Ernest and Julio Gallo" for alcoholic beverages, sued Spider Webs Ltd. for using the domain name Ernestandjuliogallo.com. Spider Webs Ltd. was a domain name speculator that owned numerous domain names consisting of famous company names. The Ernestandjuliogallo.com website contained information on the risks of alcohol use, anti-corporate articles about E. & J. Gallo Winery, and was poorly con-

structed. The court concluded that Spider Webs Ltd. was in violation of the ACPA and that its actions constituted dilution by blurring because the Ernestandjuliogallo.com domain name appeared on every page printed off the website accessed by that name, and that Spider Webs Ltd. was not free to use this particular mark as a domain name (*E. & J. Gallo Winery v. Spider Webs Ltd.*, 2001). In 2009, a court upheld the largest cybersquatting judgment to date: a $33 million verdict in favor of Verizon against OnlineNIC, an Internet domain registration company that had used over 660 names that could easily be confused with legitimate Verizon domain names. Although there have not been many cases decided under the ACPA, that does not mean the problem has gone away. Impersonation of individuals and brands on social network sites adds another dimension to the problem. Both Twitter and Facebook make cybersquatting and impersonation a violation of their terms of service.

However, it is not always easy for a firm to prevent trademark infringement by cybersquatters, or to prevent squatters from profiting from their infringing activities. In 2015, for instance, the Academy of Motion Picture Arts and Sciences (AMPAS) accused domain registrar GoDaddy of cybersquatting (*Academy of Motion Picture Arts and Sciences v. GoDaddy.com Inc et al.*, 2015). AMPAS claimed GoDaddy acted in bad faith by allowing customers to purchase 293 domain names such as Academyawards.net, Oscarsredacademyawards.net, Oscarsredcarpet.com, Billycrystal2012oscars.com, and Theoscargoestothehangover.com, and then sharing in the advertising revenues those pages generated. The court ruled that GoDaddy relied on representations of their users that their domain registrations did not infringe any trademarks, and that it took down domains after receiving takedown requests. AMPAS failed to prove intent to profit from AMPAS marks, according to the court. This suit demonstrates that trademark owners need to be vigilant in detecting infringement, sending takedown notices immediately, and following up to make sure the infringing sites are taken down. The burden is clearly on the trademark owner. The suit also demonstrates that cybersquatters have little incentive to stop trying to defraud and confuse consumers. If they are caught, their sites are taken down, but there is no penalty for trying (Stempel, 2015).

Cyberpiracy

Cyberpiracy involves the same behavior as cybersquatting, but with the intent of diverting traffic from the legitimate site to an infringing site. In *Ford Motor Co. v. Lapertosa*, Lapertosa had registered and used a website called Fordrecalls.com as an adult entertainment website. The court ruled that Fordrecalls.com was in violation of the ACPA in that it was a bad-faith attempt to divert traffic to the Lapertosa site and diluted Ford's wholesome trademark (*Ford Motor Co. v. Lapertosa*, 2001).

The Ford decision reflects two other famous cases of cyberpiracy. In the *Paine Webber Inc. v. Fortuny* case, the court enjoined Fortuny from using the domain name www.painewebber.com—a site that specialized in pornographic materials—because it diluted and tarnished Paine Webber's trademark and diverted web traffic from Paine Webber's legitimate site—Painewebber.com (*Paine Webber Inc. v. Fortuny*, 1999). In the *Playboy Enterprises, Inc. v. Global Site Designs, Inc.* case, the court enjoined the defendants from using the Playboy and Playmate marks in their domain names Playboyonline.net and Playmatesearch.net and from including the Playboy trademark in

their metatags. In these cases, the defendants' intention was diversion for financial gain (*Playboy Enterprises, Inc. v. Global Site Designs, Inc.*, 1999).

Typosquatting is a form of cyberpiracy in which a domain name contains a common misspelling of another site's name. These domains are sometimes referred to as "doppelganger" domains. Often the user ends up at a site very different from one they intended to visit. For instance, John Zuccarini is an infamous typosquatter who was jailed in 2002 for setting up pornographic websites with URLs based on misspellings of popular children's brands, such as Bob the Builder and Teletubbies. The FTC fined him again in 2007 for engaging in similar practices (McMillan, 2007). Harvard Business School professor Ben Edelman conducted a study that found that there were at least 938,000 domains typosquatting on the top 3,264 ".com" websites, and that 57% of these domains included Google pay-per click ads. In 2011, Facebook filed a lawsuit against 25 typosquatters who established websites with such domain names as Faceboook, Facemook, Faceboik, and Facebooki. In 2013, Facebook was awarded $2.8 million in damages.

Metatagging

The legal status of using famous or distinctive marks as metatags is more complex and subtle. The use of trademarks in metatags is permitted if the use does not mislead or confuse consumers. Usually this depends on the content of the site. A car dealer would be permitted to use a famous automobile trademark in its metatags if the dealer sold this brand of automobiles, but a pornography site could not use the same trademark, nor a dealer for a rival manufacturer. A Ford dealer would most likely be infringing if it used "Honda" in its metatags, but would not be infringing if it used "Ford" in its metatags. (Ford Motor Company would be unlikely to seek an injunction against one of its dealers.)

In the *Bernina of America, Inc. v. Fashion Fabrics Int'l, Inc.* case, the court enjoined Fashion Fabrics, an independent dealer of sewing machines, from using the trademarks "Bernina" and "Bernette," which belonged to the manufacturer Bernina, as metatags. The court found the defendant's site contained misleading claims about Fashion Fabrics' knowledge of Bernina products that were likely to confuse customers. The use of the Bernina trademarks as metatags per se was not a violation of ACPA, according to the court, but in combination with the misleading claims on the site would cause confusion and hence infringement (*Bernina of America, Inc. v. Fashion Fabrics Int'l, Inc.*, 2001).

In the *Nissan Motor Co., Ltd. v. Nissan Computer Corp.* case, Uzi Nissan had used his surname "Nissan" as a trade name for various businesses since 1980, including Nissan Computer Corp. Nissan.com had no relationship with Nissan Motor, but over the years began selling auto parts that competed with Nissan Motor. The court ruled that Nissan Computer's behavior did indeed infringe on Nissan Motor's trademarks, but it refused to shut the site down. Instead, the court ruled Nissan Computer could continue to use the Nissan name and metatags, but must post notices on its site that it was not affiliated with Nissan Motor (*Nissan Motor Co., Ltd. v. Nissan Computer Corp.*, 2000).

Keywording

The permissibility of using trademarks as keywords on search engines is also subtle and depends (1) on the extent to which such use is considered to be a "use in commerce" and causes "initial customer confusion" and (2) on the content of the search results.

In *Playboy Enterprises, Inc. v. Netscape Communications, Inc.*, Playboy objected to the practice of Netscape's and Excite's search engines displaying banner ads unrelated to *Playboy Magazine* when users entered search arguments such as "playboy," "playmate," and "playgirl." The Ninth Circuit Court of Appeals denied the defendant's motion for a summary judgment and held that when an advertiser's banner ad is not labeled so as to identify its source, the practice could result in trademark infringement due to consumer confusion (*Playboy Enterprises, Inc. v. Netscape Communications, Inc.*, 2004).

Google has also faced lawsuits alleging that its advertising network illegally exploits others' trademarks. For instance, insurance company GEICO challenged Google's practice of allowing competitors' ads to appear when a searcher types "Geico" as the search query. A U.S. district court ruled that this practice did not violate federal trademark laws as long as the word "Geico" was not used in the ads' text (*Government Employees Insurance Company v. Google, Inc.*, 2004). Google quickly discontinued allowing the latter, and settled the case (Associated Press, 2005). In 2009, Rosetta Stone, the language-learning software firm, filed a lawsuit against Google for trademark infringement, alleging its AdWords program allowed other companies to use Rosetta Stone's trademarks for online advertisements without permission. In 2012, the 4th Circuit Court of Appeals held that a jury might hold Google liable for trademark infringement, pointing to evidence that an internal Google study found that even sophisticated users were sometimes unaware that sponsored links were advertisements. In 2012, Rosetta Stone and Google settled, which was seen as a strategic win for Google because it eliminated one of the last major cases challenging the legitimacy of its AdWords program. Currently Google allows anyone to buy anyone else's trademark as a keyword. In 2011, Microsoft decided to follow this practice as well with Bing and Yahoo Search.

Linking

Linking refers to building hypertext links from one site to another site. This is obviously a major design feature and benefit of the Web. **Deep linking** involves bypassing the target site's home page and going directly to a content page. In *Ticketmaster Corp. v. Tickets.com*, Tickets.com—owned by Microsoft—competed directly against Ticketmaster in the events ticket market. When Tickets.com did not have tickets for an event, it would direct users to Ticketmaster's internal pages, bypassing the Ticketmaster home page. Even though its logo was displayed on the internal pages, Ticketmaster objected on the grounds that such "deep linking" violated the terms and conditions of use for its site (stated on a separate page altogether and construed by Ticketmaster as equivalent to a shrink-wrap license), and constituted false advertising, as well as the violation of copyright. The court found, however, that deep linking per se is not illegal, no violation of copyright occurred because no copies were made, the terms

linking
building hypertext links from one site to another site

deep linking
involves bypassing the target site's home page, and going directly to a content page

and conditions of use were not obvious to users, and users were not required to read the page on which the terms and conditions of use appeared in any event. The court refused to rule in favor of Ticketmaster, but left open further argument on the licensing issue. In an out-of-court settlement, Tickets.com nevertheless agreed to stop the practice of deep linking (*Ticketmaster v. Tickets.com*, 2000).

Framing

framing
involves displaying the content of another website inside your own website within a frame or window

Framing involves displaying the content of another website inside your own website within a frame or window. The user never leaves the framer's site and can be exposed to advertising while the target site's advertising is distorted or eliminated. Framers may or may not acknowledge the source of the content. In *The Washington Post, et al. v. TotalNews, Inc.,* The Washington Post Company, CNN, Reuters, and several other news organizations filed suit against TotalNews, Inc., claiming that TotalNews's use of frames on its website, TotalNews.com, infringed upon the respective plaintiffs' copyrights and trademarks, and diluted the content of their individual websites. The plaintiffs claimed additionally that TotalNews's framing practice effectively deprived the plaintiffs' websites of advertising revenue.

TotalNews's website employed four frames. The TotalNews logo appeared in the lower left frame, various links were located in a vertical frame on the left side of the screen, TotalNews's advertising was framed across the screen bottom, and the "news frame," the largest frame, appeared in the center and right. Clicking on a specific news organization's link allowed the reader to view the content of that particular organization's website, including any related advertising, within the context of the "news frame." In some instances, the framing distorted or modified the appearance of the linked website, including the advertisements, while the appearance of TotalNews's advertisements, in a separate frame, remained unchanged. In addition, the URL remained fixed on the TotalNews address, even though the content in the largest frame on the website was from the linked website. The "news frame" did not, however, eliminate the linked website's identifying features.

The case was settled out of court. The news organizations allowed TotalNews to link to their websites, but prohibited framing and any attempt to imply affiliation with the news organizations (*The Washington Post, et al. v. TotalNews, Inc.*, 1997).

TRADE SECRETS

Much of the value created by a firm lies not in copyrights, patents, or even trademarks. There is a kind of intellectual property that has to do with business procedures, formulas, and methods of manufacture and service delivery, from which the firm derives value and which it does not want to share with others in the form of a patent application or copyright application. This type of intellectual property is referred to as **trade secrets.** Most famously, the formula for Coca Cola is considered a trade secret, as are the manufacturing techniques for producing General Electric's jet engine turbine blades. Trade secrets differ from other copyright and patent protections because they may not be unique or novel. Information in a firm can be considered a trade secret if (a) it is a secret (something that others do not know), (b)

trade secret
information that is secret, has commercial value, and has been protected by its owner

Determining how or whether personal information should be retained or deleted on the Internet is just one of many ethical, social, and political issues raised by the rapid evolution of the Internet and e-commerce. For instance, as discussed in the opening case, whether individuals lose control over all personal information once it is placed on the Internet is still up for debate in the United States. In Europe, in contrast, individuals do retain rights to their personal information. These questions are not just ethical questions that we as individuals have to answer; they also involve social institutions such as family, schools, business firms, and in some cases, entire nation-states. And these questions have obvious political dimensions because they involve collective choices about how we should live and what laws we would like to live under.

In this chapter, we discuss the ethical, social, and political issues raised in e-commerce, provide a framework for organizing the issues, and make recommendations for managers who are given the responsibility of operating e-commerce companies within commonly accepted standards of appropriateness.

8.1 UNDERSTANDING ETHICAL, SOCIAL, AND POLITICAL ISSUES IN E-COMMERCE

The Internet and its use in e-commerce have raised pervasive ethical, social, and political issues on a scale unprecedented for computer technology. Entire sections of daily newspapers and weekly magazines are devoted to the social impact of the Internet. But why is this so? Why is the Internet at the root of so many contemporary controversies? Part of the answer lies in the underlying features of Internet technology itself, and the ways in which it has been exploited by business firms. Internet technology and its use in e-commerce disrupt existing social and business relationships and understandings.

Consider for instance Table 1.2 (in Chapter 1), which lists the unique features of Internet technology. Instead of considering the business consequences of each unique feature, **Table 8.1** examines the actual or potential ethical, social, and/or political consequences of the technology.

We live in an "information society," where power and wealth increasingly depend on information and knowledge as central assets. Controversies over information are often disagreements over power, wealth, influence, and other things thought to be valuable. Like other technologies, such as steam, electricity, telephones, and television, the Internet and e-commerce can be used to achieve social progress, and for the most part, this has occurred. However, the same technologies can be used to commit crimes, despoil the environment, and threaten cherished social values. Before automobiles, there was very little interstate crime and very little federal jurisdiction over crime. Likewise with the Internet: before the Internet, there was very little "cybercrime."

Many business firms and individuals are benefiting from the commercial development of the Internet, but this development also exacts a price from individuals, organizations, and societies. These costs and benefits must be carefully considered by those seeking to make ethical and socially responsible decisions in this new envi-

TABLE 8.1 UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY AND THEIR POTENTIAL ETHICAL, SOCIAL, AND/OR POLITICAL IMPLICATIONS

E-COMMERCE TECHNOLOGY DIMENSION	POTENTIAL ETHICAL, SOCIAL, AND POLITICAL SIGNIFICANCE
Ubiquity—Internet/web technology is available everywhere: at work, at home, and elsewhere via mobile devices, anytime.	Work and shopping can invade family life; shopping can distract workers at work, lowering productivity; use of mobile devices can lead to automobile and industrial accidents. Presents confusing issues of "nexus" to taxation authorities.
Global reach—The technology reaches across national boundaries, around the Earth.	Reduces cultural diversity in products; weakens local small firms while strengthening large global firms; moves manufacturing production to low-wage areas of the world; weakens the ability of all nations—large and small—to control their information destiny.
Universal standards—There is one set of technology standards, namely Internet standards.	Increases vulnerability to viruses and hacking attacks worldwide, affecting millions of people at once. Increases the likelihood of "information" crime, crimes against systems, and deception.
Richness—Video, audio, and text messages are possible.	A "screen technology" that reduces use of text and potentially the ability to read by focusing instead on video and audio messages. Potentially very persuasive messages that may reduce reliance on multiple independent sources of information.
Interactivity—The technology works through interaction with the user.	The nature of interactivity at commercial sites can be shallow and meaningless. Customer e-mails are frequently not read by human beings. Customers do not really "co-produce" the product as much as they "co-produce" the sale. The amount of "customization" of products that occurs is minimal, occurring within predefined platforms and plug-in options.
Information density—The technology reduces information costs, and raises quality.	While the total amount of information available to all parties increases, so does the possibility of false and misleading information, unwanted information, and invasion of solitude. Trust, authenticity, accuracy, completeness, and other quality features of information can be degraded. The ability of individuals and organizations to make sense out of this plethora of information is limited.
Personalization/Customization—The technology allows personalized messages to be delivered to individuals as well as groups.	Opens up the possibility of intensive invasion of privacy for commercial and governmental purposes that is unprecedented.
Social technology—The technology enables user content generation and social networking.	Creates opportunities for cyberbullying, abusive language, and predation; challenges concepts of privacy, fair use, and consent to use posted information; creates new opportunities for surveillance by authorities and corporations into private lives.

ronment. The question is: How can you as a manager make reasoned judgments about what your firm should do in a number of e-commerce areas—from securing the privacy of your customer's clickstream to ensuring the integrity of your company's domain name?

A MODEL FOR ORGANIZING THE ISSUES

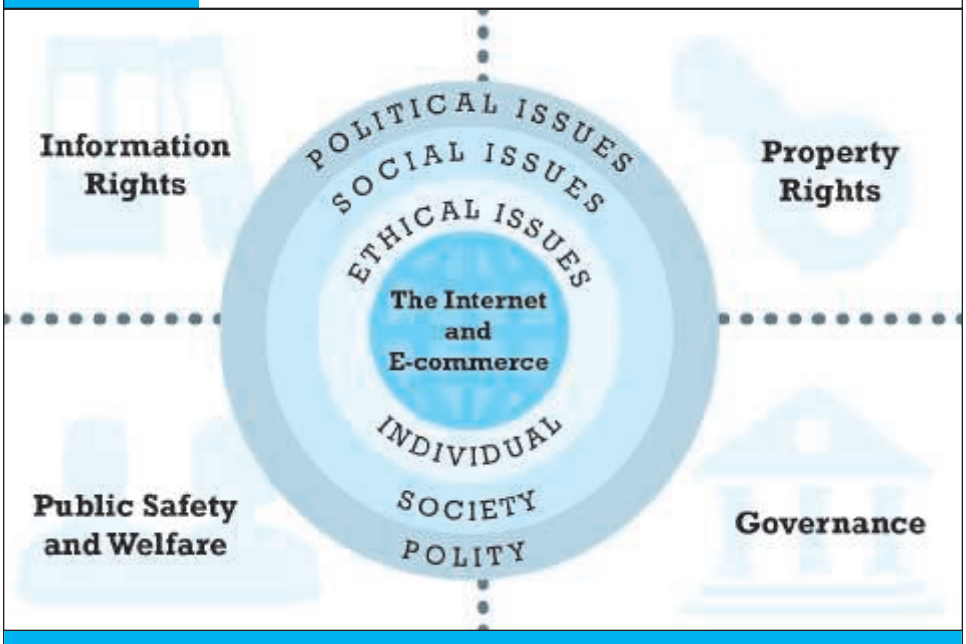
E-commerce—and the Internet—have raised so many ethical, social, and political issues that it is difficult to classify them all, and hence, complicated to see their relationship to one another. Clearly, ethical, social, and political issues are interrelated. One way to organize the ethical, social, and political dimensions surrounding

e-commerce is shown in **Figure 8.1**. At the individual level, what appears as an ethical issue—"What should I do?"—is reflected at the social and political levels—"What should we as a society and government do?" The ethical dilemmas you face as a manager of a business using the Web reverberate and are reflected in social and political debates. The major ethical, social, and political issues that have developed around e-commerce over the past 10 years can be loosely categorized into four major dimensions: information rights, property rights, governance, and public safety and welfare.

Some of the ethical, social, and political issues raised in each of these areas include the following:

- **Information rights:** What rights to their own personal information do individuals have in a public marketplace, or in their private homes, when Internet technologies make information collection so pervasive and efficient? What rights do individuals have to access information about business firms and other organizations?
- **Property rights:** How can traditional intellectual property rights be enforced in an Internet world where perfect copies of protected works can be made and easily distributed worldwide in seconds?
- **Governance:** Should the Internet and e-commerce be subject to public laws? And if so, what law-making bodies have jurisdiction—state, federal, and/or international?

FIGURE 8.1 THE MORAL DIMENSIONS OF AN INTERNET SOCIETY



The introduction of the Internet and e-commerce impacts individuals, societies, and political institutions. These impacts can be classified into four moral dimensions: property rights, information rights, governance, and public safety and welfare.

- **Public safety and welfare:** What efforts should be undertaken to ensure equitable access to the Internet and e-commerce channels? Should governments be responsible for ensuring that schools and colleges have access to the Internet? Are certain online content and activities—such as pornography, gambling, or anonymous tweeting of hateful language—a threat to public safety and welfare? What about connected cars? Should mobile commerce be allowed from moving vehicles?

To illustrate, imagine that at any given moment, society and individuals are more or less in an ethical equilibrium brought about by a delicate balancing of individuals, social organizations, and political institutions. Individuals know what is expected of them, social organizations such as business firms know their limits, capabilities, and roles, and political institutions provide a supportive framework of market regulation, banking, and commercial law that provides sanctions against violators.

Now, imagine we drop into the middle of this calm setting a powerful new technology such as the Internet and e-commerce. Suddenly, individuals, business firms, and political institutions are confronted by new possibilities of behavior. For instance, individuals discover that they can download perfect digital copies of music tracks from websites without paying anyone, something that, under the old technology of CDs, would have been impossible. This can be done, despite the fact that these music tracks still legally belong to the owners of the copyright—musicians and record label companies. Then, business firms discover that they can make a business out of aggregating these digital musical tracks—or creating a mechanism for sharing musical tracks—even though they do not "own" them in the traditional sense. The record companies, courts, and Congress were not prepared at first to cope with the onslaught of online digital copying. Courts and legislative bodies will have to make new laws and reach new judgments about who owns digital copies of copyrighted works and under what conditions such works can be "shared." It may take years to develop new understandings, laws, and acceptable behavior in just this one area of social impact. In the meantime, as an individual and a manager, you will have to decide what you and your firm should do in legal "gray" areas, where there is conflict between ethical principles but no clear-cut legal or cultural guidelines. How can you make good decisions in this type of situation?

Before examining the four moral dimensions of e-commerce in greater depth, we will briefly review some basic concepts of ethical reasoning that you can use as a guide to ethical decision making, and provide general reasoning principles about the social and political issues of the Internet that you will face in the future.

BASIC ETHICAL CONCEPTS: RESPONSIBILITY, ACCOUNTABILITY, AND LIABILITY

Ethics is at the heart of social and political debates about the Internet. **Ethics** is the study of principles that individuals and organizations can use to determine right and wrong courses of action. It is assumed in ethics that individuals are free moral agents who are in a position to make choices. When faced with alternative courses of action, what is the correct moral choice? Extending ethics from individuals to business firms and even entire societies can be difficult, but it is not impossible. As long as there is

ethics
the study of principles that individuals and organizations can use to determine right and wrong courses of action

a decision-making body or individual (such as a board of directors or CEO in a business firm, or a governmental body in a society), their decisions can be judged against a variety of ethical principles.

If you understand some basic ethical principles, your ability to reason about larger social and political debates will be improved. In western culture, there are four basic principles that all ethical schools of thought share: responsibility, accountability, liability, and due process. **Responsibility** means that as free moral agents, individuals, organizations, and societies are responsible for the actions they take. **Accountability** means that individuals, organizations, and societies should be held accountable to others for the consequences of their actions. The third principle—liability—extends the concepts of responsibility and accountability to the area of law. **Liability** is a feature of political systems in which a body of law is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. **Due process** is a feature of law-governed societies and refers to a process in which laws are known and understood, and there is an ability to appeal to higher authorities to ensure that the laws have been correctly applied.

responsibility
as free moral agents, individuals, organizations, and societies are responsible for the actions they take

accountability
individuals, organizations, and societies should be held accountable to others for the consequences of their actions

liability
a feature of political systems in which a body of law is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations

due process
a process in which laws are known and understood and there is an ability to appeal to higher authorities to ensure that the laws have been correctly applied

You can use these concepts immediately to understand some contemporary Internet debates. For instance, consider the 2005 U.S. Supreme Court decision in the case of *Metro-Goldwyn-Mayer Studios v. Grokster, et al.* MGM had sued Grokster and other P2P networks for copyright infringement. The court decided that because the primary and intended use of Internet P2P file-sharing services such as Grokster, StreamCast, and Kazaa was the swapping of copyright-protected music and video files, the file-sharing services should be held accountable and shut down. Although Grokster and the other networks acknowledged that the most common use of the software was for illegal digital music file-swapping, they argued that there were substantial, nontrivial uses of the same networks for legally sharing files. They also argued they should not be held accountable for what individuals do with their software, any more than Sony could be held accountable for how people use VCRs, or Xerox for how people use copying machines. Ultimately, the Supreme Court ruled that Grokster and other P2P networks could be held accountable for the illegal actions of their users if it could be shown that they intended their software to be used for illegal downloading and sharing, and had marketed the software for that purpose. The court relied on copyright laws to arrive at its decisions, but these laws reflect some basic underlying ethical principles of responsibility, accountability, and liability.

Underlying the *Grokster* Supreme Court decision is a fundamental rejection of the notion that the Internet is an ungoverned "Wild West" environment that cannot be controlled. Under certain defined circumstances, the courts will intervene into the uses of the Internet. No organized civilized society has ever accepted the proposition that technology can flaunt basic underlying social and cultural values. Through all of the industrial and technological developments that have taken place, societies have intervened by means of legal and political decisions to ensure that the technology serves socially acceptable ends without stifling the positive consequences of innovation and wealth creation. The Internet in this sense is no different, and we can expect societies around the world to exercise more regulatory control over the

Internet and e-commerce in an effort to arrive at a new balance between innovation and wealth creation, on the one hand, and other socially desirable objectives on the other. This is a difficult balancing act, and reasonable people will arrive at different conclusions.

ANALYZING ETHICAL DILEMMAS

Ethical, social, and political controversies usually present themselves as dilemmas. A **dilemma** is a situation in which there are at least two diametrically opposed actions, each of which supports a desirable outcome. When confronted with a situation that seems to present an ethical dilemma, how can you analyze and reason about the situation? The following is a five-step process that should help:

dilemma
a situation in which there are at least two diametrically opposed actions, each of which supports a desirable outcome

1. **Identify and clearly describe the facts.** Find out who did what to whom, and where, when, and how. In many instances, you will be surprised at the errors in the initially reported facts, and often you will find that simply getting the facts straight helps define the solution. It also helps to get the opposing parties involved in an ethical dilemma to agree on the facts.
2. **Define the conflict or dilemma and identify the higher-order values involved.** Ethical, social, and political issues always reference higher values. Otherwise, there would be no debate. The parties to a dispute all claim to be pursuing higher values (e.g., freedom, privacy, protection of property, and the free enterprise system). For example, supporters of the use of advertising networks such as DoubleClick argue that the tracking of consumer movements on the Web increases market efficiency and the wealth of the entire society. Opponents argue this claimed efficiency comes at the expense of individual privacy, and advertising networks should cease their activities or offer web users the option of not participating in such tracking.
3. **Identify the stakeholders.** Every ethical, social, and political issue has stakeholders: players in the game who have an interest in the outcome, who have invested in the situation, and usually who have vocal opinions. Find out the identity of these groups and what they want. This will be useful later when designing a solution.
4. **Identify the options that you can reasonably take.** You may find that none of the options satisfies all the interests involved, but that some options do a better job than others. Sometimes, arriving at a "good" or ethical solution may not always be a balancing of consequences to stakeholders.
5. **Identify the potential consequences of your options.** Some options may be ethically correct but disastrous from other points of view. Other options may work in this one instance but not in other similar instances. Always ask yourself, "What if I choose this option consistently over time?"

Once your analysis is complete, you can refer to the following well-established ethical principles to help decide the matter.

CANDIDATE ETHICAL PRINCIPLES

Although you are the only one who can decide which ethical principles you will follow and how you will prioritize them, it is helpful to consider some ethical principles with deep roots in many cultures that have survived throughout recorded history:

- **The Golden Rule:** Do unto others as you would have them do unto you. Putting yourself into the place of others and thinking of yourself as the object of the decision can help you think about fairness in decision making.
- **Universalism:** If an action is not right for all situations, then it is not right for any specific situation (Immanuel Kant's categorical imperative). Ask yourself, "If we adopted this rule in every case, could the organization, or society, survive?"
- **Slippery Slope:** If an action cannot be taken repeatedly, then it is not right to take at all. An action may appear to work in one instance to solve a problem, but if repeated, would result in a negative outcome. In plain English, this rule might be stated as "once started down a slippery path, you may not be able to stop."
- **Collective Utilitarian Principle:** Take the action that achieves the greater value for all of society. This rule assumes you can prioritize values in a rank order and understand the consequences of various courses of action.
- **Risk Aversion:** Take the action that produces the least harm, or the least potential cost. Some actions have extremely high failure costs of very low probability (e.g., building a nuclear generating facility in an urban area) or extremely high failure costs of moderate probability (speeding and automobile accidents). Avoid the high-failure cost actions and choose those actions whose consequences would not be catastrophic, even if there were a failure.
- **No Free Lunch:** Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise. (This is the ethical "no free lunch" rule.) If something someone else has created is useful to you, it has value and you should assume the creator wants compensation for this work.
- **The New York Times Test (Perfect Information Rule):** Assume that the results of your decision on a matter will be the subject of the lead article in the *New York Times* the next day. Will the reaction of readers be positive or negative? Would your parents, friends, and children be proud of your decision? Most criminals and unethical actors assume imperfect information, and therefore they assume their decisions and actions will never be revealed. When making decisions involving ethical dilemmas, it is wise to assume perfect information markets.
- **The Social Contract Rule:** Would you like to live in a society where the principle you are supporting would become an organizing principle of the entire society? For instance, you might think it is wonderful to download illegal copies of Hollywood movies, but you might not want to live in a society that does not respect property rights, such as your property rights to the car in your driveway, or your rights to a term paper or original art.

None of these rules is an absolute guide, and there are exceptions and logical difficulties with all of them. Nevertheless, actions that do not easily pass these guidelines

deserve some very close attention and a great deal of caution because the appearance of unethical behavior may do as much harm to you and your company as the actual behavior.

Now that you have an understanding of some basic ethical reasoning concepts, let's take a closer look at each of the major types of ethical, social, and political debates that have arisen in e-commerce.

8.2 PRIVACY AND INFORMATION RIGHTS

Privacy is arguably the most complex ethical issue raised by e-commerce, as well as the changing technology of human communications brought on by the Internet and mobile devices. It may be the most delicate and vexing issue of our digital age, one that will continue to evolve through this century. How can we square the ever-growing power of digital technologies to gather personal information by businesses and government with the notion that individuals have the right to be left alone, free to think what they want without fear?

In ways not anticipated by technologists or politicians, these digital technologies and devices have become the primary means of personal interaction with other people and firms. The smartphone and Internet are now at the center of social, political, and business life. In the fast-growing online marketplace for goods and services, these technologies efficiently and faithfully record human market behavior in ways never imagined. The resulting trove of personal private information gathered by online merchants has no precedent in history. Laws and regulations to govern the use of this information are weak and poorly defined. As a result, consumers often feel they have lost control over their personal information online. And, indeed, they have.

privacy
the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state

information privacy
subset of privacy that rests on four central premises, including the moral rights to control use of information collected and to know whether information is being collected, the right to personal information due process, and the right to have personal information stored in a secure manner

right to be forgotten
the claim of individuals to be able to edit and delete personal information

WHAT IS PRIVACY?

The claim to **privacy** rests on the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Privacy is one girder supporting freedom: without the privacy required to think, write, plan, and associate independently and without fear, social and political freedom is weakened, and perhaps destroyed.

Information privacy is a subset of privacy that rests on four central premises. First, individuals have a moral right to be able to control the use of whatever information is collected about them, whether or not they consented to the gathering of information in the first place. Individuals should be able to edit, delete, and shape the use of their online personal information by governments and business firms. In this view, individuals even have the "**right to be forgotten**," as discussed in the opening case (Rosen, 2012).

Second, individuals have a moral right to know when information is being collected about them, and must give their consent prior to collecting their personal information. This is the principle of "informed consent," that people are rational actors who

are informed, and who will make their own choices in the marketplace, including the decision whether to give their information in return for some benefit.

Third, individuals have a right to personal information due process. The process of collecting, sharing, disseminating personal information must be "fair" and transparent to everyone. Systems of personal information—whether public or private—must be publicly known (no secret systems), operate according to a published set of rules (terms of use policies) describing how governments and firms will use personal information, and define ways in which people can edit, correct, and shape their personal information in a system of records.

Fourth, individuals have a right to have their personal information stored in a secure manner. Personal record systems must have procedures in place to protect personal information from intrusion, hacking, and unauthorized uses.

These principles of personal information privacy are reflected in a doctrine called Fair Information Practices (FIP), established by the Federal Trade Commission (FTC) in 2000 (see **Table 8.2**). We discuss the role of the FTC in protecting personal private information further later in the chapter.

PRIVACY IN THE PUBLIC SECTOR: PRIVACY RIGHTS OF CITIZENS

The concept and practice of privacy, and its legal foundation, are very different in the public versus the private sector. In the public sector, concepts of privacy have a long history that has evolved over two centuries of court rulings, laws, and regulations in the United States and Europe. In the private sector, concepts of privacy are much more recent, and in the age of the Internet, in a state of flux, debate, and argument.

TABLE 8.2 THE FTC'S FAIR INFORMATION PRACTICE PRINCIPLES

Notice/Awareness (core principle)	Sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/inactive), voluntary or required, consequences of refusal, and steps taken to protect confidentiality, integrity, and quality of the data.
Choice/Consent (core principle)	There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties. Opt-in/opt-out must be available.
Access/Participation	Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security	Data collectors must take reasonable steps to assure that consumer information is accurate and secure from unauthorized use.
Enforcement	There must be a mechanism to enforce FIP principles in place. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulation.

SOURCES: Based on data from Federal Trade Commission, 1998, 2000.