

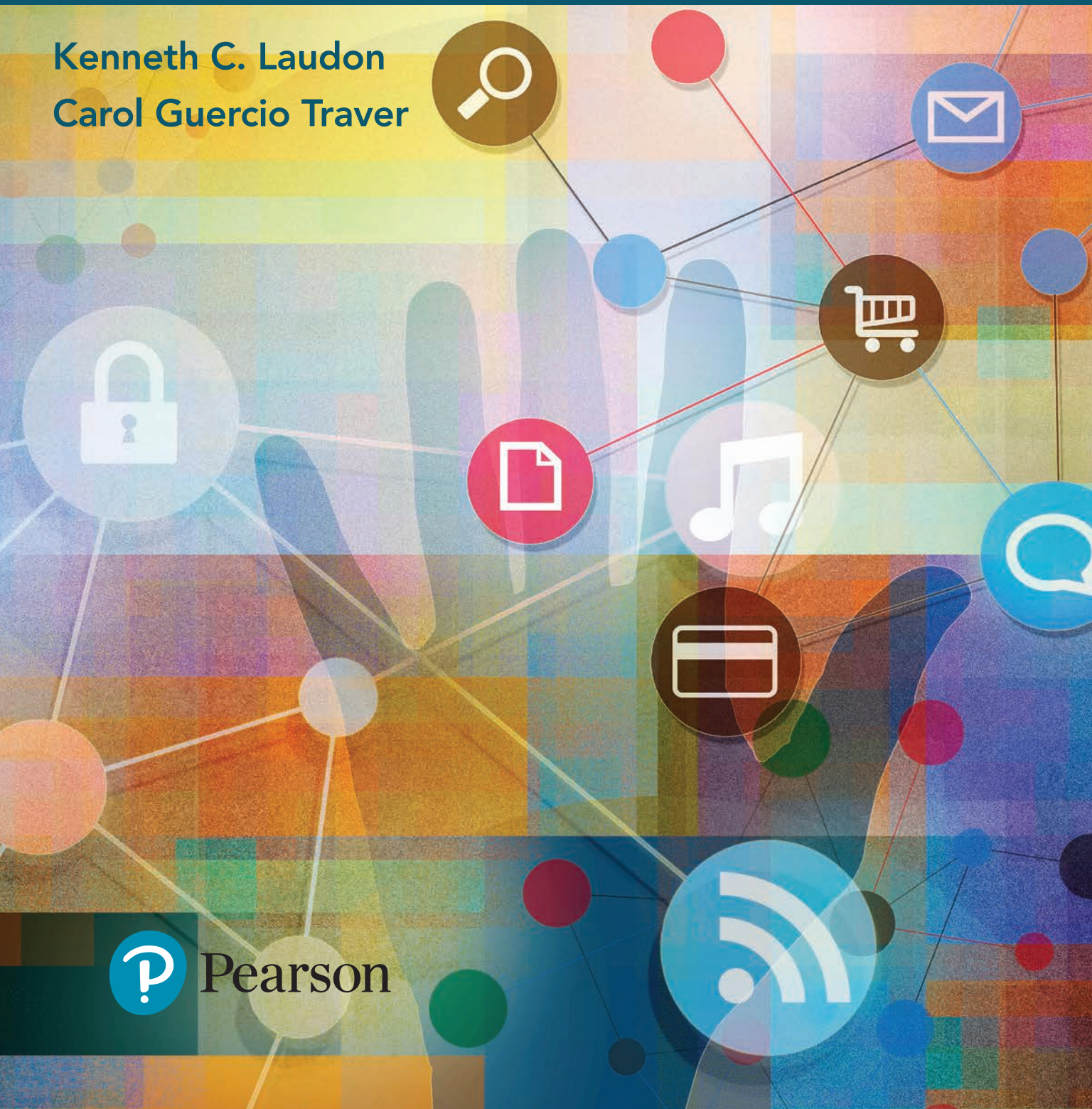
E-commerce

business. technology. society.

2017

THIRTEENTH EDITION

Kenneth C. Laudon
Carol Guercio Traver



 Pearson

PART

1



- **CHAPTER 1**
The Revolution Is Just Beginning
- **CHAPTER 2**
E-commerce Business Models and Concepts

Introduction to E-commerce



CHAPTER

1

The Revolution Is Just Beginning

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Understand why it is important to study e-commerce.
- Define e-commerce, understand how e-commerce differs from e-business, identify the primary technological building blocks underlying e-commerce, and recognize major current themes in e-commerce.
- Identify and describe the unique features of e-commerce technology and discuss their business significance.
- Describe the major types of e-commerce.
- Understand the evolution of e-commerce from its early years to today.
- Describe the major themes underlying the study of e-commerce.
- Identify the major academic disciplines contributing to e-commerce.

Uber:

The New Face of E-commerce?

If you were trying to pick iconic examples of e-commerce in the two decades since it began in 1995, it is likely that companies such as Amazon, eBay, Google, Apple, and Facebook would be high on the list. Today, there's a new company that is becoming the face of e-commerce as it enters its third decade: Uber. Uber and other firms with similar business models, such as Lyft (a ride service similar to Uber's), Airbnb (rooms for rent), Heal (doctor home visits), Handy (part-time household helpers), Instacart (grocery shopping), Washio (laundry service), and BloomThat (flower delivery), are the pio-



© Lenscap/Alamy

رواد
neers of a new on-demand service e-commerce business model that is sweeping up billions of investment dollars and disrupting major industries, from transportation to hotels, real estate, house cleaning, maintenance, and grocery shopping. On-demand service firms have collected over \$26 billion in venture capital funding over the last five years, making this the hottest business model in e-commerce.

Uber offers a variety of different services. The two most common are UberX, which uses compact sedans and is the least expensive, and UberBlack, which provides higher-priced town car service. UberPool is a ride-sharing service that allows users to share a ride with another person who happens to be going to the same place. In several cities, Uber is developing UberEats, a food delivery service; UberRush, a same-day delivery service; and UberCargo, a trucking service.

Uber, headquartered in San Francisco, was founded in 2009 by Travis Kalanick and Garrett Camp, and has grown explosively since then to over 480 cities in 69 countries. Drivers are signing up at an exponential rate: as of the beginning of 2016, there were over 450,000 drivers in the United States and over 1 million worldwide. According to an Uber-sponsored survey, over 44% of Uber drivers have college degrees (compared to 15% of taxi drivers), 71% say they have boosted their income and financial security by driving for Uber, and 73% say they prefer a job where they choose their hours rather than a 9-to-5 job. It is estimated that Uber's revenue will reach around \$2 billion in 2016, but it is still not expected to generate an overall profit, with losses in developing markets

Types of Uber?

6 Types of Uber:

such as China and India swallowing up profits being generated in North America, Europe, and elsewhere. **Uber's strategy** is to expand as fast as possible while foregoing short-term profits in the hope of long-term returns. As of July 2016, Uber has raised over \$12.5 billion in venture capital. Uber is currently valued at around \$68 billion, more than all of its competitors combined. In August 2016, Uber agreed to sell Uber China, where it had been engaged in a costly turf war for Chinese riders, to Didi Chuxing Technology, its primary Chinese rival. Uber will receive a 18% interest in Didi Chuxing and Didi will invest \$1 billion in Uber. In doing so, Uber converted a reported \$2 billion loss on its Chinese operations into a new merged entity valued at around \$7 billion, and freed up capital to invest more heavily in other emerging markets such as Indonesia and India where it does not have such significant competition. **1** **2**

Uber's Strategy

Uber offers a compelling value proposition for both customers and drivers. Customers can sign up for free, request and pay for a ride (at a cost Uber claims is 40% less than a traditional taxi) using a smartphone and credit card, and get picked up within a few minutes. No need to stand on a street corner frantically waving, competing with others, or waiting and waiting for an available cab to drive by, without knowing when that might happen. Instead, customers using the Uber app know just how long it will take for the ride to arrive and how much it will cost. With UberPool ride-sharing, the cost of a ride drops by 50%, making it cost-competitive with owning a car in an urban area, according to Uber. **Uber's value proposition for drivers** is that it allows them to set their own hours, work when they like, and put their own cars to use generating revenue.

Uber's Value Proposition

Uber is the current poster child for "digital disruption." It is easy to see why Uber has ignited a firestorm of opposition from existing taxi services both in the United States and around the world. Who can compete in a market where a new upstart firm offers a 50% price reduction? If you've paid \$1 million for a license to drive a taxi in New York City, what is it worth now that Uber has arrived? **Even governments find Uber to be a disruptive threat.** Governments do not want to give up regulatory control over passenger safety, driver training, nor the healthy revenue stream generated by charging taxi firms for a taxi license and sales taxes.

Uber's business model differs from traditional retail e-commerce. Uber doesn't sell goods. Instead it has created a smartphone-based platform that enables people who want a service—like a taxi—to find a provider with the resources, such as a personal automobile and a driver with available time, to fill the demand. It's important to understand that although Uber and similar firms are often called "sharing economy" companies, this is a misnomer. **Uber drivers are selling their services as drivers** and the temporary use of their car. Uber itself is not in the sharing business either: it charges a hefty fee for every transaction on its platform. **Uber is not an example of true "peer-to-peer" e-commerce because Uber transactions involve an online intermediary: a third party that takes a cut of all transactions and arranges for the marketplace to exist in the first place.**

Uber's Business Model

inaccurate name

huge

Taxi=cab

Uber has disrupted the traditional taxi business model because it offers a superior, fast, convenient taxi-hailing service when compared to traditional taxi companies. **With a traditional taxi service, there is no guarantee you will find a cab.** Uber reduces that uncertainty: the customer enters a request for pickup using his or her smartphone and

nearly instantly (under the best of circumstances), Uber finds a provider and notifies the customer of the estimated time of arrival and price. Riders can accept the price or find an alternative.

Uber's business model is much more efficient than a traditional taxi firm. Uber does not own taxis and has no maintenance and financing costs. Uber calls its drivers "independent contractors," not employees. Doing so enables Uber to avoid costs for workers' compensation, minimum wage requirements, driver training, health insurance, and commercial licensing.

Uber's business model is much more efficient than a traditional taxi firm ?? Why

Quality control would seem to be a nightmare with over 1 million contract drivers. But Uber relies on user reviews to identify problematic drivers and driver reviews to identify problematic passengers. Drivers are evaluated by riders on a 5-point scale. Drivers that fall below 4.5 are warned and may be dropped if they don't improve. Customers are also rated with a 5-point system. Drivers can refuse to pick up troublesome customers, and the Uber server can delay service to potential customers with low ratings or ban them entirely. Uber does not publicly report how many poorly rated drivers or passengers there are in its system. Academic articles have found that in similar on-demand companies, such as Airbnb, there is a built-in bias for both sellers and buyers to give good reviews regardless of the actual experience. If you routinely give low reviews to sellers (drivers), they will think you are too demanding and not service you in the future. If a driver gives low reviews to passengers, they might not rate you highly in return.

Quality control

Rather than having a dispatcher in every city, Uber has an Internet-based app service running on cloud servers located throughout the world. It does not provide radios to its drivers, who instead must use their own smartphones and cell service, which the drivers pay for. It does not provide insurance or maintenance for its drivers' cars. Uber has shifted the costs of running a taxi service entirely to the drivers. Uber charges prices that vary dynamically with demand: the higher the demand, the greater the price of a ride. Therefore, it is impossible using public information to know if Uber's prices are lower than traditional taxis. Clearly, in high-demand situations they are higher, sometimes ten times higher, than a regulated taxi. There is no regulatory taxi commission setting uniform per mile fares. Consumers do face some traditional uncertainties regarding availability: during a rain storm, a convention, or a sports event, when demand peaks, not enough drivers may be available at any price.

If Uber is the poster child for the new on-demand service economy, it's also an iconic example of the social costs and conflicts associated with this new kind of e-commerce. Uber has been accused by attorney generals in several states of misclassifying its drivers as contractors as opposed to employees, thereby denying the drivers the benefits of employee status, such as minimum wages, social security, workers' compensation, and health insurance. In June 2015, the California Labor Commission ruled that an Uber driver was, in fact, an employee under the direct, detailed supervision and control of Uber management, notwithstanding Uber's claims that it merely provides a "platform." However, the ruling applied only to that individual driver, and Uber is appealing the decision. In April 2016, Uber settled two federal class action lawsuits brought in California and Massachusetts on behalf of an estimated 385,000 drivers, who sued the company for mistreatment and

SOURCES: "Uber Driver Settlement Rejected, Both Parties Resume Negotiations," by Robert Lawson, *Norcalrecord.com*, October 12, 2016; "Even Uber Couldn't Bridge the China Divide," by Farhad Manjoo, *New York Times*, August 1, 2016; "Uber Sells China Operations to Didi Chuxing," by Alyssa Abkowitz and Rick Carew, *Wall Street Journal*, August 1, 2016; "Why Uber Keeps Raising Billions," by Andrew Ross Sorkin, *New York Times*, June 20, 2016; "Uber Points to Profits in All Developed Markets," by Leslie Hook, *FT.com*, June 16, 2016; "An Uber Shakedown," *Wall Street Journal*, April 24, 2016; "Uber Settlement Takes Customers For a Ride," by Rob Berger, *Forbes*, April 22, 2016; "Uber Settles Cases With Concessions, but Drivers Stay Freelancers," by Mike Isaac and Noam Scheiber, *New York Times*, April 21, 2016; "Leaked: Uber's Financials Show Huge Growth, Even Bigger Losses," by Brian Solomon, *Forbes*, January 12, 2016; "Twisting Words to Make 'Sharing' Apps Seem Selfless," by Natasha Singer, *New York Times*, August 9, 2015; "Uber Dealt Setback on Labor Rules," by Lauren Weber, *Wall Street Journal*, June 18, 2015; "The \$50 Billion Question: Can Uber Deliver?," by Douglas Macmillan, *Wall Street Journal*, June 15, 2015; "How Everyone Misjudges the Sharing Economy," by Christopher Mims, *Wall Street Journal*, May 25, 2015; "The On-Demand Economy Is Reshaping Companies and Careers," *The Economist*, January 4, 2015; "The On-Demand Economy: Workers on Tap," *The Economist*, January 3, 2015.

lack of due process, including barring them from the app without explanation, lack of transparency in how driver ratings are calculated, and deactivating drivers who regularly declined to accept requests. Uber agreed to pay up to \$84 million to the drivers, give them more information about why they are barred from using the app, assist drivers in forming "driver associations" in these two states, and review its policy of no tipping. Uber also agreed to pay an additional \$16 million if it goes public next year with a valuation exceeding \$93.75 billion. The company retained the right to shut out drivers temporarily if their acceptance rates are low and can deactivate drivers completely if they have high cancellation rates. Most importantly, the settlement allowed Uber to continue classifying its drivers as independent contractors in California and Massachusetts, enabling Uber to continue not paying for workers' compensation insurance, health insurance, or overtime work. However, in August 2016, a federal district court judge in California rejected the terms of the settlement on the grounds that it was unfair and unreasonable, and as a result, Uber and the parties to the lawsuit have resumed negotiations. The terms on which the lawsuit are finally resolved may have a significant effect on the on-demand services business model.

Uber has also been accused of violating public transportation laws and regulations throughout the United States and the world; abusing the personal information it has collected on users of the service; seeking to use personal information to intimidate journalists; failing to protect public safety by refusing to do adequate criminal, medical, and financial background checks on its drivers; taking clandestine actions against its chief competitor Lyft in order to disrupt its business; and being tone-deaf to the complaints of its own drivers against the firm's efforts to reduce driver fees. Uber has been banned in several European cities.

Critics also fear the long-term impact of on-demand service firms, because of their potential for creating a society of part-time, low-paid, temp work, displacing traditionally full-time, secure jobs—the so-called "uberization" of work. As one critic put it, Uber is not the Uber for rides so much as it is the Uber for low-paid jobs. Uber responds to this fear by claiming that it is lowering the cost of transportation, making better use of spare human and financial resources, expanding the demand for ride services, and expanding opportunities for car drivers, whose pay is about the same as other taxi drivers.

Despite the controversy surrounding it, Uber continues to have no trouble attracting additional investors and according to CEO Kalanick, plans to remain a private company for the foreseeable future. Although Uber currently has a host of rivals, both big and small, most analysts expect that ultimately, only one or two major players will remain. Uber is doing everything it can to assure that it will be the one to prevail.

In 1994, e-commerce as we now know it did not exist. In 2016, just 22 years later, around 177 million American consumers are expected to spend about \$600 billion, and businesses around \$6.7 trillion, purchasing goods, services, and digital content via a desktop computer or mobile device. A similar story has occurred throughout the world. And in this short period of time, e-commerce has been reinvented not just once, but twice.

The early years of e-commerce, during the late 1990s, were a period of business vision, inspiration, and experimentation. It soon became apparent, however, that establishing a successful business model based on those visions would not be easy. There followed a period of retrenchment and reevaluation, which led to the stock market crash of 2000–2001, with the value of e-commerce, telecommunications, and other technology stocks plummeting. After the bubble burst, many people were quick to write off e-commerce. But they were wrong. The surviving firms refined and honed their business models, and the technology became more powerful and less expensive, ultimately leading to business firms that actually produced profits. Between 2002–2008, retail e-commerce grew at more than 25% per year.

Today, we are in the middle of yet another transition. Social networks such as Facebook, Twitter, YouTube, Pinterest, Instagram, and Tumblr, which enable users to distribute their own content (such as videos, music, photos, personal information, commentary, blogs, and more), have rocketed to prominence. Never before in the history of media have such large audiences been aggregated and made so accessible. At the same time, mobile devices, such as smartphones and tablet computers, and mobile apps have supplanted the traditional desktop/laptop platform and web browser as the most common method for consumers to access the Internet. Facilitated by technologies such as cloud computing, cellular networks, and Wi-Fi, mobile devices have become advertising, shopping, reading, and media viewing machines, and in the process, are transforming consumer behavior yet again. Mobile, social, and local have become driving forces in e-commerce. The mobile platform infrastructure has also given birth to yet another e-commerce innovation: on-demand services that are local and personal. From hailing a taxi, to shopping, to washing your clothes, these new businesses are creating a marketplace where owners of resources such as cars, spare bedrooms, and spare time can find a market of eager consumers looking to buy a service in a few minutes using their smartphones. Uber, profiled in the opening case, is a leading example of these new on-demand service firms that are disrupting traditional business models.

1.1 THE FIRST THIRTY SECONDS: WHY YOU SHOULD STUDY E-COMMERCE

The rapid growth and change that has occurred in the first two decades of e-commerce represents just the beginning—what could be called the first 30 seconds of the e-commerce revolution. Technology continues to evolve at exponential rates. This

انکماش

fall or drop
straight
down at
high speed

underlying ferment presents entrepreneurs with new opportunities to create new business models and businesses in traditional industries and in the process, disrupt, and in some instances, destroy existing business models and firms.

Improvements in underlying information technologies and continuing entrepreneurial innovation in business and marketing promise as much change in the next decade as was seen in the previous two decades. The twenty-first century will be the age of a digitally enabled social and commercial life, the outlines of which we can still only barely perceive at this time. Analysts estimate that by 2020, consumers will be spending around \$933 billion and businesses around \$9.1 trillion in digital transactions. It appears likely that e-commerce will eventually impact nearly all commerce, and that most commerce will be e-commerce by the year 2050, if not sooner.

Business fortunes are made—and lost—in periods of extraordinary change such as this. The next five years hold exciting opportunities—as well as risks—for new and traditional businesses to exploit digital technology for market advantage. For society as a whole, the next few decades offer the possibility of extraordinary gains in social wealth as the digital revolution works its way through larger and larger segments of the world's economy.

It is important to study e-commerce in order to be able to perceive and understand the opportunities and risks that lie ahead. By the time you finish this book, you will be able to identify the technological, business, and social forces that have shaped, and continue to shape, the growth of e-commerce, and be ready to participate in, and ultimately guide, discussions of e-commerce in the firms where you work. More specifically, you will be able to analyze an existing or new idea for an e-commerce business, identify the most effective business model to use, and understand the technological underpinnings of an e-commerce presence, including the security and ethical issues raised, as well as how to optimally market and advertise the business, using both traditional e-marketing tools and social, mobile, and local marketing.

1

2

4

5

7

3

6

Why we should study E-commerce?

1.2 INTRODUCTION TO E-COMMERCE

In this section, we'll first define e-commerce and then discuss the difference between e-commerce and e-business. We will also introduce you to the major technological building blocks underlying e-commerce: the Internet, Web, and mobile platform. The section concludes with a look at some major current trends in e-commerce.

WHAT IS E-COMMERCE?

E-commerce involves the use of the Internet, the World Wide Web (Web), and mobile apps and browsers running on mobile devices to transact business. Although the terms Internet and Web are often used interchangeably, they are actually two very different things. The Internet is a worldwide network of computer networks, and the Web is one of the Internet's most popular services, providing access to billions of web pages. An app (short-hand for application) is a software application. The term is typically used when referring to mobile applications, although it is also sometimes used to refer to desktop computer applications as well. A mobile browser is a version of web browser

e-commerce

the use of the Internet, the Web, and mobile apps and browsers running on mobile devices to transact business. More formally, digitally enabled commercial transactions between and among organizations and individuals

software accessed via a mobile device. (We describe the Internet, Web, and mobile platform more fully later in this chapter and in Chapters 3 and 4.) More formally, e-commerce can be defined as digitally enabled commercial transactions between and among organizations and individuals. Each of these components of our working definition of e-commerce is important. *Digitally enabled transactions* include all transactions mediated by digital technology. For the most part, this means transactions that occur over the Internet, the Web, and/or via mobile devices. *Commercial transactions* involve the exchange of value (e.g., money) across organizational or individual boundaries in return for products and services. *Exchange of value* is important for understanding the limits of e-commerce. Without an exchange of value, no commerce occurs.

The professional literature sometimes refers to e-commerce as digital commerce. For our purposes, we consider *e-commerce* and *digital commerce* to be synonymous.

THE DIFFERENCE BETWEEN E-COMMERCE AND E-BUSINESS

There is a debate about the meaning and limitations of both e-commerce and e-business. Some argue that e-commerce encompasses the entire world of electronically based organizational activities that support a firm's market exchanges—including a firm's entire information system infrastructure (Rayport and Jaworski, 2003). Others argue, on the other hand, that e-business encompasses the entire world of internal and external electronically based activities, including e-commerce (Kalakota and Robinson, 2003).

We think it is important to make a working distinction between e-commerce and e-business because we believe they refer to different phenomena. *E-commerce is not* “anything digital” that a firm does. For purposes of this text, we will use the term **e-business** to refer primarily to the digital enabling of transactions and processes *within* a firm, involving information systems under the control of the firm. For the most part, in our view, *e-business* does not include *commercial transactions* involving an *exchange of value* across organizational boundaries. For example, a company's online inventory control mechanisms are a component of e-business, but such internal processes do not directly generate revenue for the firm from outside businesses or consumers, as e-commerce, by definition, does. It is true, however, that a firm's *e-business infrastructure* provides support for *online e-commerce exchanges*; the same *infrastructure and skill sets* are involved in both e-business and e-commerce. E-commerce and e-business systems blur together at the business firm boundary, at the point where internal business systems link up with suppliers or customers (see **Figure 1.1**). E-business applications turn into e-commerce precisely when an *exchange of value* occurs (see Mesenbourg, U.S. Department of Commerce, 2001, for a similar view). We will examine this intersection further in Chapter 12.

TECHNOLOGICAL BUILDING BLOCKS UNDERLYING E-COMMERCE: THE INTERNET, WEB, AND MOBILE PLATFORM

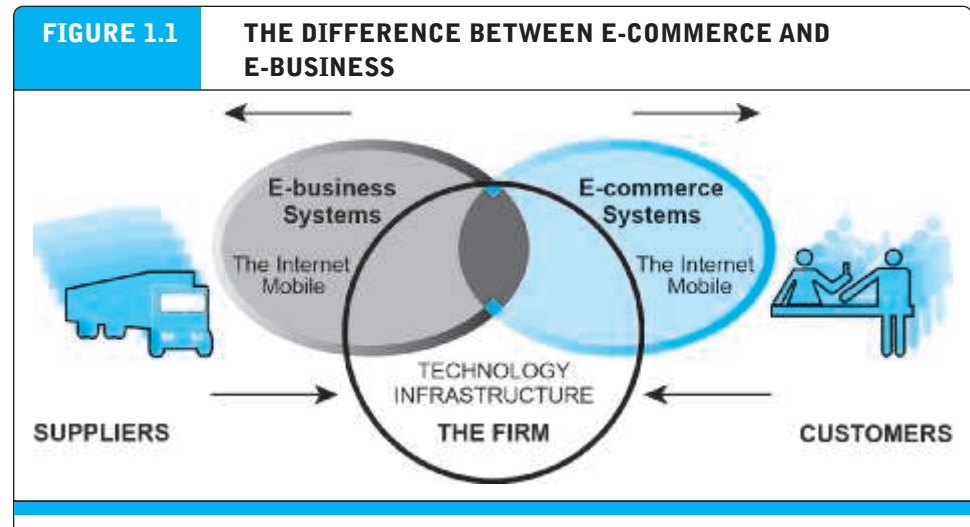
The technology juggernauts behind e-commerce are the *Internet*, the *Web*, and increasingly, the *mobile platform*. We describe the Internet, Web, and mobile platform in some detail in Chapter 3. The **Internet** is a worldwide network of computer networks built on common standards. Created in the late *1960s* to connect a small number of

e-business

the digital enabling of transactions and processes within a firm, involving information systems under the control of the firm

Internet

worldwide network of computer networks built on common standards



E-commerce primarily involves transactions that cross firm boundaries. E-business primarily involves the application of digital technologies to business processes within the firm.

mainframe computers and their users, the Internet has since grown into the world's largest network. It is impossible to say with certainty exactly how many computers and other mobile devices such as smartphones and tablets are connected to the Internet worldwide at any one time, but some experts estimate the number to be more than 5 billion (Camhi, 2015). The Internet links businesses, educational institutions, government agencies, and individuals together, and provides users with services such as e-mail, document transfer, shopping, research, instant messaging, music, videos, and news.

One way to measure the growth of the Internet is by looking at the number of Internet hosts with domain names. (An *Internet host* is defined by the Internet Systems Consortium as any IP address that returns a domain name in the in-addr.arpa domain, which is a special part of the DNS namespace that resolves IP addresses into domain names.) In January 2016, there were more than 1 billion Internet hosts in over 245 countries, up from just 70 million in 2000 (Internet Systems Consortium, 2016).

The Internet has shown extraordinary growth patterns when compared to other electronic technologies of the past. It took radio 38 years to achieve a 30% share of U.S. households. It took television 17 years to achieve a 30% share. It took only 10 years for the Internet/Web to achieve a 53% share of U.S. households once a graphical user interface was invented for the Web in 1993. Today, in the United States, around 267 million people of all ages (about 82% of the U.S. population) use the Internet at least once a month (eMarketer, Inc. 2016a).

The **World Wide Web (the Web)** is an information system that runs on the Internet infrastructure. The Web was the original “killer app” that made the Internet commercially interesting and extraordinarily popular. The Web was developed in the early 1990s and hence is of much more recent vintage than the Internet. We describe

World Wide Web (the Web)

an information system running on Internet infrastructure that provides access to billions of web pages

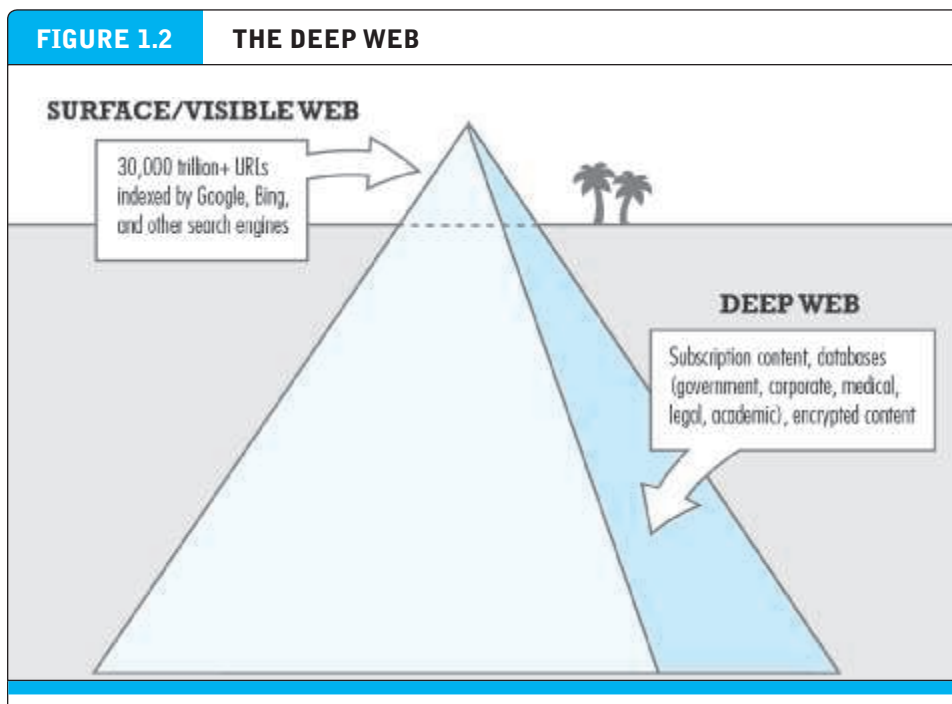
the Web in some detail in Chapter 3. The Web provides access to billions of web pages indexed by Google and other search engines. These pages are created in a language called *HTML (HyperText Markup Language)*. HTML pages can contain text, graphics, animations, and other objects. The Internet prior to the Web was primarily used for text communications, file transfers, and remote computing. The Web introduced far more powerful and commercially interesting capabilities of direct relevance to commerce. In essence, the Web added color, voice, and video to the Internet, creating a communications infrastructure and information storage system that rivals television, radio, magazines, and libraries.

There is no precise measurement of the number of web pages in existence, in part because today's search engines index only a portion of the known universe of web pages. Google has identified over 30,000 trillion unique uniform resource locators (URLs), commonly known as web addresses, up from 1 trillion in 2008, although many of these pages do not necessarily contain unique content (Schwartz, 2015). In addition to this "surface" or "visible" Web, there is also the so-called deep Web that is reportedly 500 to 1,000 times greater than the surface Web. The deep Web contains databases and other content that is not routinely indexed by search engines such as Google (see Figure 1.2). Although the total size of the Web is not known, what is indisputable is that web content has grown exponentially since 1993.

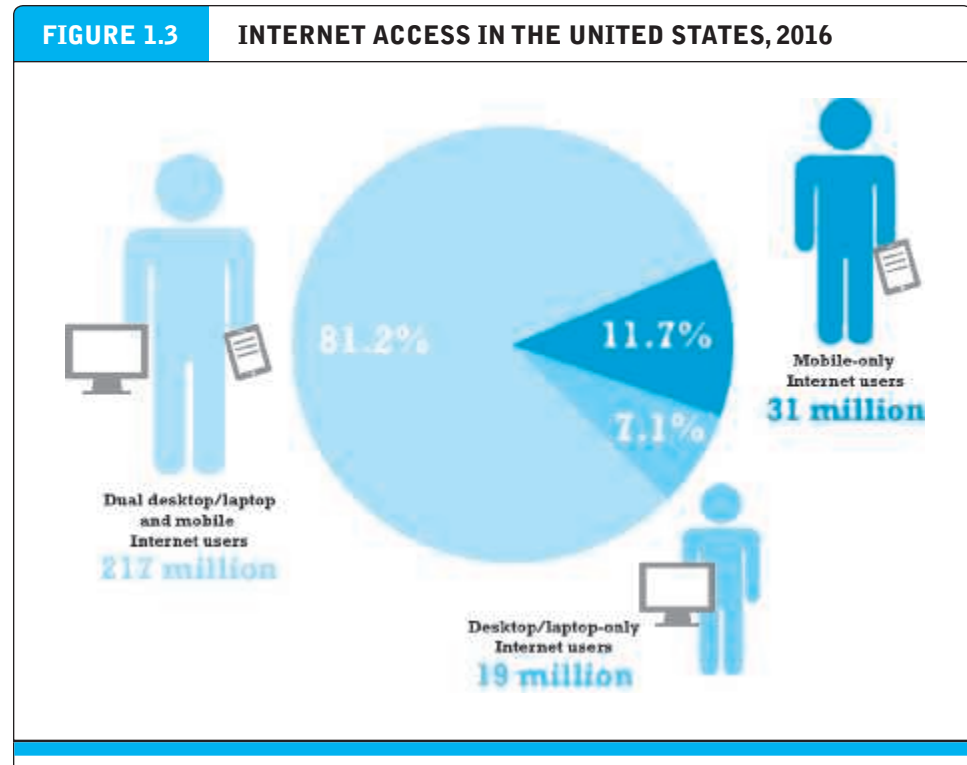
The mobile platform is the newest development in Internet infrastructure. The mobile platform provides the ability to access the Internet from a variety of mobile

mobile platform

provides the ability to access the Internet from a variety of mobile devices such as smartphones, tablets, and other ultra-lightweight laptop computers



Search engines index only a small portion of online content.



Over 80% of all Internet users in the United States (217 million people) go online using both a desktop/laptop and mobile device. Almost 12% (31 million) only go online by using a mobile device. Just over 7% (19 million) use only a desktop or laptop computer to access the Internet.


SOURCE: Based on data from eMarketer, Inc., 2016c.

devices such as smartphones, tablets, and other ultra-lightweight laptop computers via wireless networks or cell phone service. Mobile devices are playing an increasingly prominent role in Internet access. In 2016, there are over 360 million mobile devices in the United States that can be connected to the Internet (more than 1 device for each person in the United States), and almost 93% of Americans who access the Internet use a mobile device to do so at least some of the time (eMarketer, Inc., 2016b, 2016c). **Figure 1.3** illustrates the variety of devices used by Americans to access the Internet in 2016.

The mobile platform is not just a hardware phenomenon. The introduction of the Apple iPhone in 2007, followed by the Apple iPad in 2010, has also ushered in a sea-change in the way people interact with the Internet from a software perspective. In the early years of e-commerce, the Web and web browsers were the only game in town. Today, in contrast, more Americans access the Internet via a mobile app than by using a desktop computer and web browser. *Insight on Technology: Will Apps Make the Web Irrelevant?* examines the challenge that apps and the mobile platform pose to the Web's dominance of the Internet ecosphere in more depth.

INSIGHT ON TECHNOLOGY

WILL APPS MAKE THE WEB IRRELEVANT?



Nowadays, it's hard to recall a time before the Web. How did we get along without the ability to pull up a web browser and search for any item, learn about any topic, or play just about any type of game? Though the Web has come a remarkably long way from its humble beginnings, many experts claim that the Web's best days are behind it, and that there's a new player on the field: apps. Opinions vary widely over the future role of the Web in a world where apps have become an ever larger portion of the Internet marketplace. In 10 years, will web browsers be forgotten relics, as we rely entirely on apps to do both our work and our play on the Internet? Will the Web and apps coexist peacefully as vital cogs in the Internet ecosystem? Or will the app craze eventually die down as tech users gravitate back toward the Web as the primary way to perform Internet-related tasks?

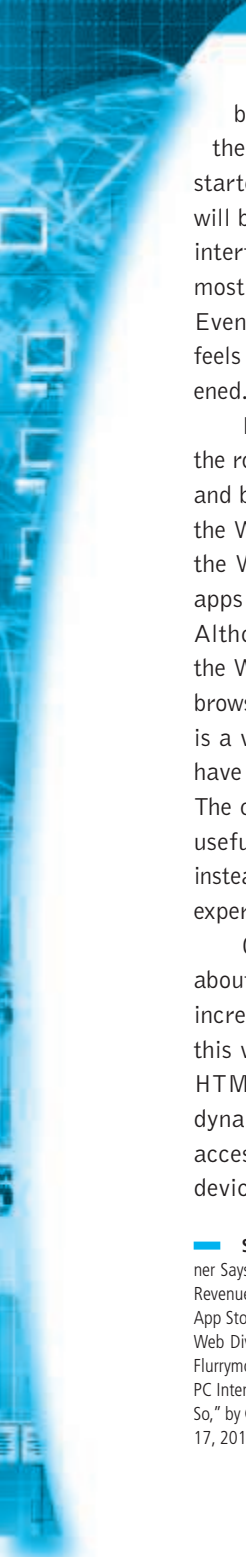
Apps have grown into a disruptive force ever since Apple launched its App Store in 2008. The list of industries apps have disrupted is wide-ranging: communications, media and entertainment, logistics, education, healthcare, and most recently, with Uber, the taxi industry. Despite not even existing prior to 2008, in 2016, sales of apps are expected to account for over \$59 billion in revenues worldwide, and the app economy is continuing to show robust growth, with estimates of over \$100 billion in revenue by 2020. More of those revenues are likely to come from in-app purchases than from paid app downloads. Not only that, but the growth is not coming from more users trying the same small number of apps. Although usage of apps tends to be highly concentrated, with nearly 75% of smartphone app minutes spent on an individual's top 3 apps, consumers are trying new apps all the time and visit about 27 apps per month, leaving plenty of room

for new app developers to innovate and create best-selling apps. In fact, according to mobile advertising company Flurry, 280 million people worldwide qualify as mobile addicts, which they define as someone who launches a smartphone app more than 60 times a day. According to Flurry, the number of such addicts increased by about 350% from 2013 to 2015.

In January 2014, for the first time ever, Americans used mobile apps more than desktop computers to access the Internet. The time U.S. adults are spending using mobile apps has exploded, growing by over 110% over the past three years, and now accounting for 58% of total digital media time spent; time spent on the desktop now accounts for just 33%, and mobile browsers just 9%. U.S. adults are spending over 96 hours a month (about 3¼ hours a day) within apps on their smartphones and tablet computers. Consumers have gravitated to apps for several reasons. First, smartphones and tablet computers enable users to use apps anywhere, instead of being tethered to a desktop or having to lug a heavy laptop around. Of course, smartphones and tablets enable users to use the Web too, but apps are often more convenient and boast more streamlined, elegant interfaces than mobile web browsers.

Not only are apps more appealing in certain ways to consumers, they are much more appealing to content creators and media companies. Apps are much easier to control and monetize than websites, not to mention they can't be crawled by Google or other services. On the Web, the average price of ads per thousand impressions is falling, and many content providers are still mostly struggling to turn the Internet into a profitable content delivery platform. Much of software and media companies' focus has shifted to developing mobile apps for this reason.

(continued)



These trends are why some pundits boldly proclaim that the Web is dead, and that the shift from the Web to apps has only just started. These analysts believe that the Internet will be used to transport data, but individual app interfaces will replace the web browser as the most common way to access and display content. Even the creator of the Web, Tim Berners-Lee, feels that the Web as we know it is being threatened. That's not a good sign.

But there is no predictive consensus about the role of the Web in our lives in the next decade and beyond. Many analysts believe the demise of the Web has been greatly exaggerated, and that the Web boasts many advantages over today's apps that users will be unwilling to relinquish. Although apps may be more convenient than the Web in many respects, the depth of the web browsing experience trumps that of apps. The Web is a vibrant, diverse array of sites, and browsers have an openness and flexibility that apps lack. The connections between websites enhance their usefulness and value to users, and apps that instead seek to lock users in cannot offer the same experience.

Other analysts who are more optimistic about the Web's chances to remain relevant in an increasingly app-driven online marketplace feel this way because of the emergence of HTML5. HTML5 is a markup language that enables more dynamic web content and allows for browser-accessible web apps that are as appealing as device-specific apps. In fact, there is another

group of analysts who believe that apps and the Web are going to come together, with HTML5 bringing the best of the app experience to the Web, and with apps developing new web-like capabilities. Already, work is underway to create more "smart" apps that handle a wider array of tasks than today's apps can handle, such as apps with Siri integration.

A shift towards apps and away from the Web could have a ripple effect on e-commerce firms. As the pioneer of apps and the market leader in apps, smartphones, and tablet computers, Apple stands to gain from a shift towards apps, and although it also faces increasing competition from other companies, including Google, the established success of the App Store will make it next to impossible to dethrone Apple. For instance, while Google's Google Play store had double the number of downloads compared to Apple's App Store in 2015, the App Store still made 75% more revenue than Google Play. Google's search business is likely to suffer from all of the "walled garden" apps that it cannot access, but it also has a major stake in the world of smartphones, tablets, and apps itself with its Android operating system, which is used by over 80% of smartphones worldwide. Facebook has already seen its members make the transition from using its website to using its mobile app and has made, and continues to make, significant investments in standalone apps, such as Instagram and WhatsApp. Web-based companies that fail to find an answer to the growth of mobile apps may eventually fall by the wayside.

— **SOURCES:** "The 2016 U.S. Mobile App Report," comScore, September 2016; "US Mobile StatPack," by Cathy Boyle, eMarketer, March 2016; "Gartner Says Worldwide Smartphone Sales Grew 9.7 Percent in Fourth Quarter of 2015," Gartner.com, February 18, 2016; "App Forecast: Over \$100 Billion in Revenue by 2020," by Danielle Levitas, Blog.Appannie.com, February 10, 2016; "App Annie 2015: Google Play Saw 100% More Downloads Than the iOS App Store, but Apple Generated 75% More Revenue," by Emil Protalinski, Venturebeat.com, January 20, 2016; "Publisher Straddle the Apple-Google, App-Web Divide," by Katie Benner and Conor Dougherty, *New York Times*, October 18, 2015; "Mobile Addicts Multiply Across the Globe," by Simon Khalaf, Flurrymobile.tumblr.com, July 15, 2015; "How Apps Won the Mobile Web," by Thomas Claburn, Informationweek.com, April 3, 2014; "Mobile Apps Overtake PC Internet Usage in U.S.," by James O'Toole, Money.cnn.com, February 28, 2014; "Is The Web Dead In the Face of Native Apps? Not Likely, But Some Think So," by Gabe Knuth, Brianmadden.com, March 28, 2012; "The Web Is Dead. Long Live the Internet," by Chris Anderson and Michael Wolff, Wired.com, August 17, 2010; "The Web Is Dead? A Debate," by Chris Anderson, Wired.com, August 17, 2010.

MAJOR TRENDS IN E-COMMERCE

Table 1.1 describes the major trends in e-commerce in 2016–2017 from a business, technological, and societal perspective, the three major organizing themes that we use in this book to understand e-commerce (see Section 1.6).

From a business perspective, one of the most important trends to note is that all forms of e-commerce continue to show very strong growth. Retail e-commerce has been growing at double-digit rates for the last few years, and by 2017, is expected to reach \$460 billion, while mobile e-commerce is anticipated to increase by almost 30% to around \$232 billion. Social networks such as Facebook, Pinterest, and Instagram are enabling social e-commerce by providing advertising, search, and Buy buttons that enable consumers to actually purchase products. Local e-commerce is being fueled by the explosion of interest in on-demand services such as Uber and Airbnb. B2B e-commerce, which dwarfs all other forms, also is continuing to strengthen and grow.

From a technology perspective, the mobile platform based on smartphones and tablet computers has finally arrived with a bang, driving astronomical growth in mobile advertising and making true mobile e-commerce a reality. The use of mobile messaging services such as WhatsApp and Snapchat has created an alternative communications platform that are beginning to be leveraged for commerce as well. Cloud computing is inextricably linked to the development of the mobile platform by enabling the storage of consumer content and software on cloud (Internet-based) servers, and making it available to mobile devices as well as desktops. Other major technological trends include the increasing ability of companies to track and analyze the flood of online data (typically referred to as big data) being produced. The Internet of Things, comprised of billions of Internet-connected devices, continues to grow exponentially, and will only add to this flood of data in the years to come.

At the societal level, other trends are apparent. The Internet and mobile platform provide an environment that allows millions of people to create and share content, establish new social bonds, and strengthen existing ones through social network, photo- and video-posting, and blogging sites and apps, while at the same time creating significant privacy issues. Privacy seems to have lost some of its meaning in an age when millions create public online personal profiles, while at the same time concerns over commercial and governmental privacy invasion continue to increase. The major digital copyright owners have increased their pursuit of online piracy with mixed success, while reaching agreements with the big technology players such as Apple, Amazon, and Google to protect intellectual property rights. Governments have successfully moved toward taxation of e-commerce sales. Sovereign nations have expanded their surveillance of, and control over, online communications and content as a part of their anti-terrorist activities and their traditional interest in law enforcement. Online security, or lack thereof, remains a significant issue, as new stories about security breaches, malware, hacking, and other attacks emerge seemingly daily.

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

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

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

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

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.

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 marketplace, 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.**

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.

reach

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

universal standards

standards that are shared by all nations around the world

What are the three benefits of universal standards?

richness

the complexity and content of a message

interactivity

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

INTERACTIVITY

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.

Name three of the business consequences that can be result from growth in information density?

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.

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.

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

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

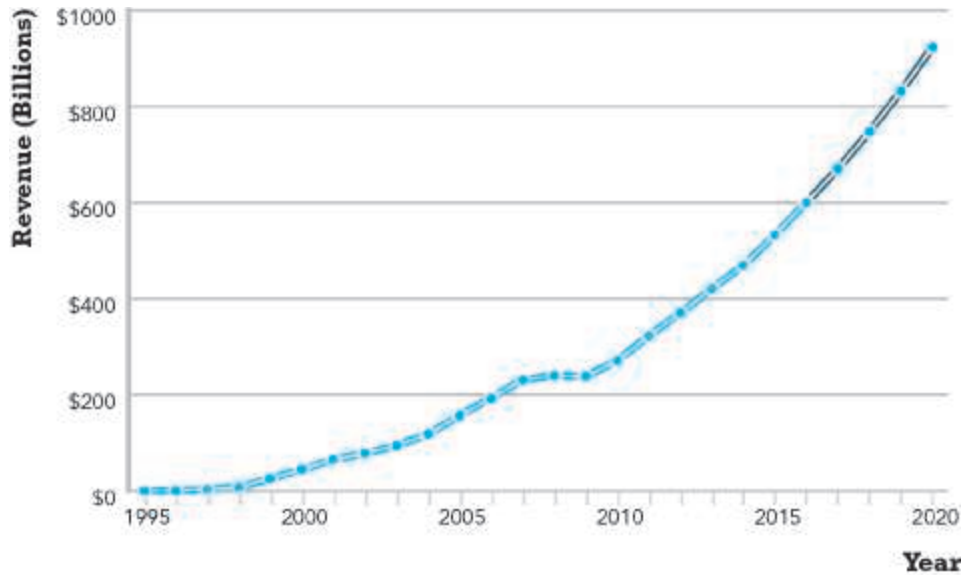
business-to-consumer (B2C) e-commerce
online businesses selling to individual consumers

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.

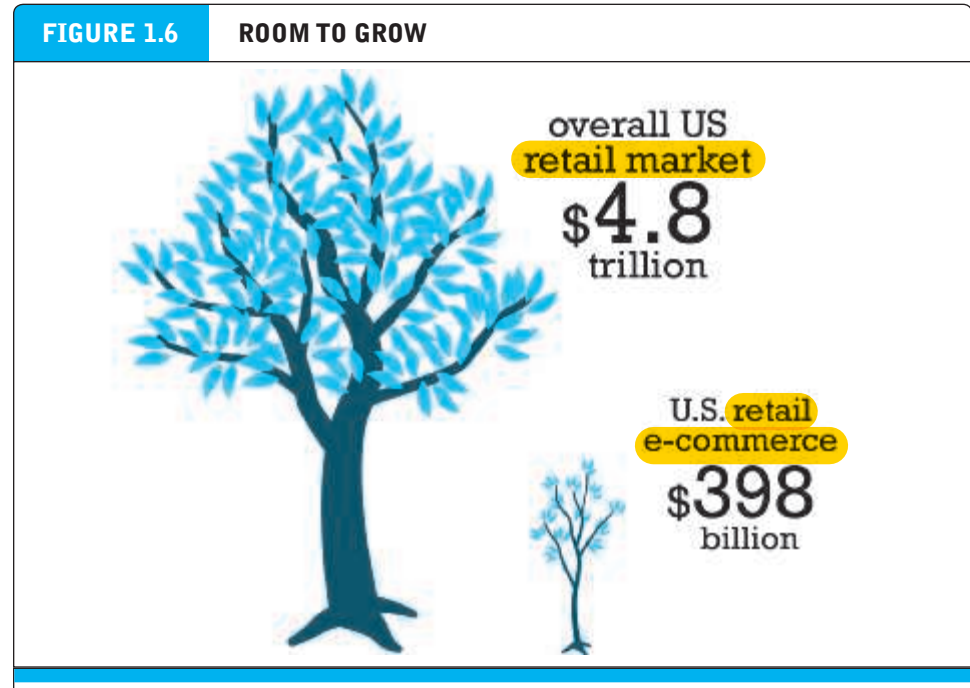
The data suggests that, over the next five years, B2C e-commerce in the United States will grow by over 10% annually. There is tremendous upside potential. Today, for instance, retail e-commerce (which currently comprises the lion's share of B2C e-commerce revenues) is still a very small part (around 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, in which businesses focus on selling to other businesses, is the largest form of e-commerce, with around \$6.7 trillion in

business-to-business (B2B) e-commerce

online businesses selling to other businesses



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

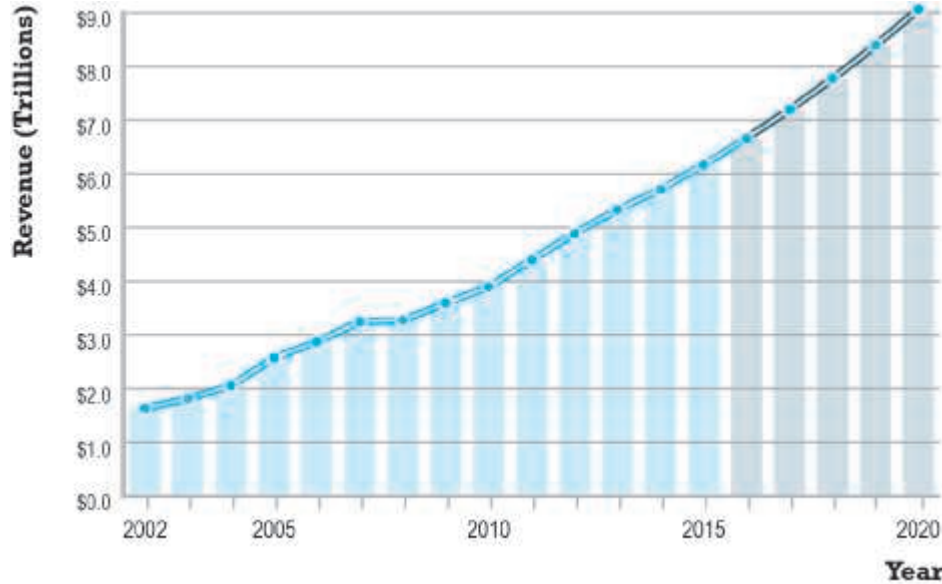
consumer-to-consumer (C2C) e-commerce
consumers selling to other consumers

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.

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

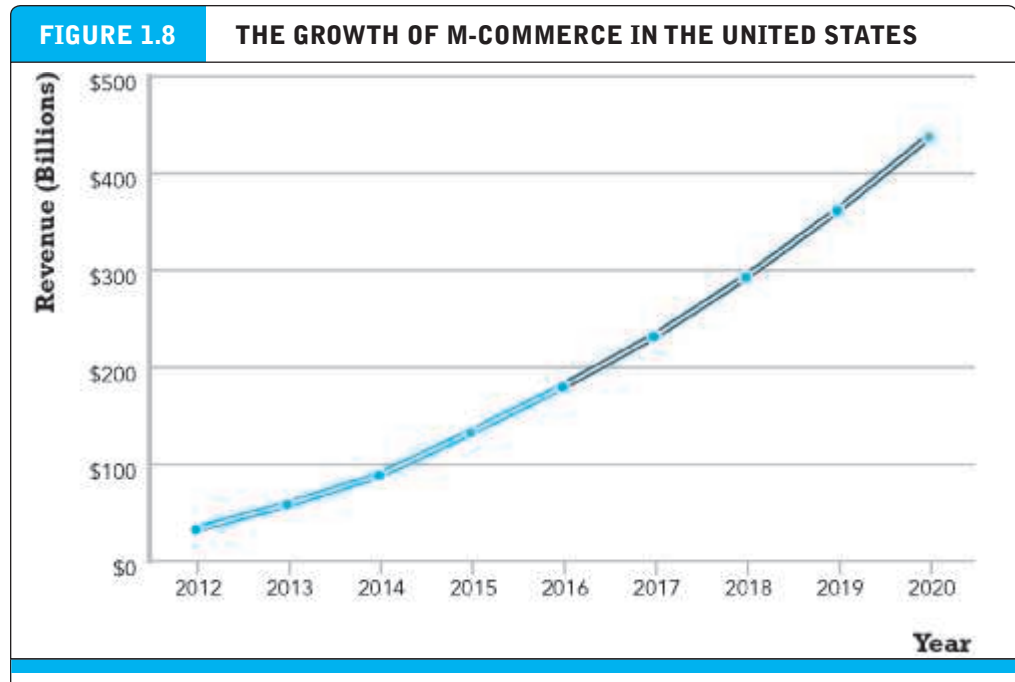
Social e-commerce is e-commerce that is enabled by social networks and online social relationships. The growth of social e-commerce is being driven by a number of factors, including the increasing popularity of social sign-on (signing onto websites using your Facebook or other social network ID), network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

mobile e-commerce (m-commerce)

use of mobile devices to enable online transactions

social e-commerce

e-commerce enabled by social networks and online social relationships



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).

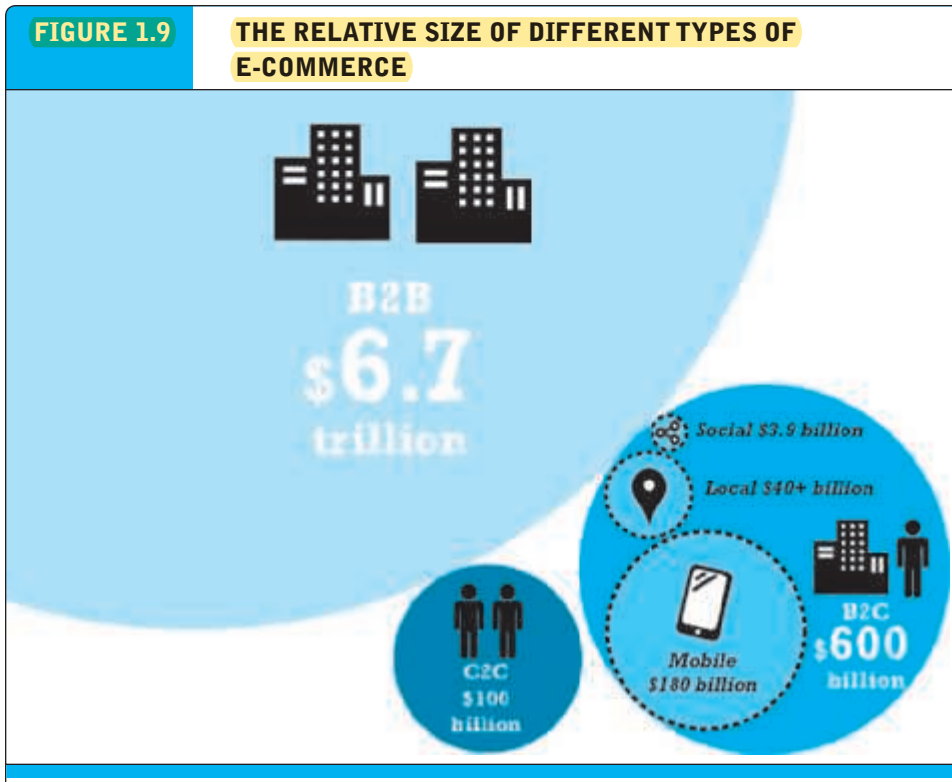
Social e-commerce is often intertwined with m-commerce, particularly as more and more social network users access those networks via mobile devices. A variation of social e-commerce known as *conversational commerce* leverages the mobile connection even further. Conversational commerce involves the use 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.



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

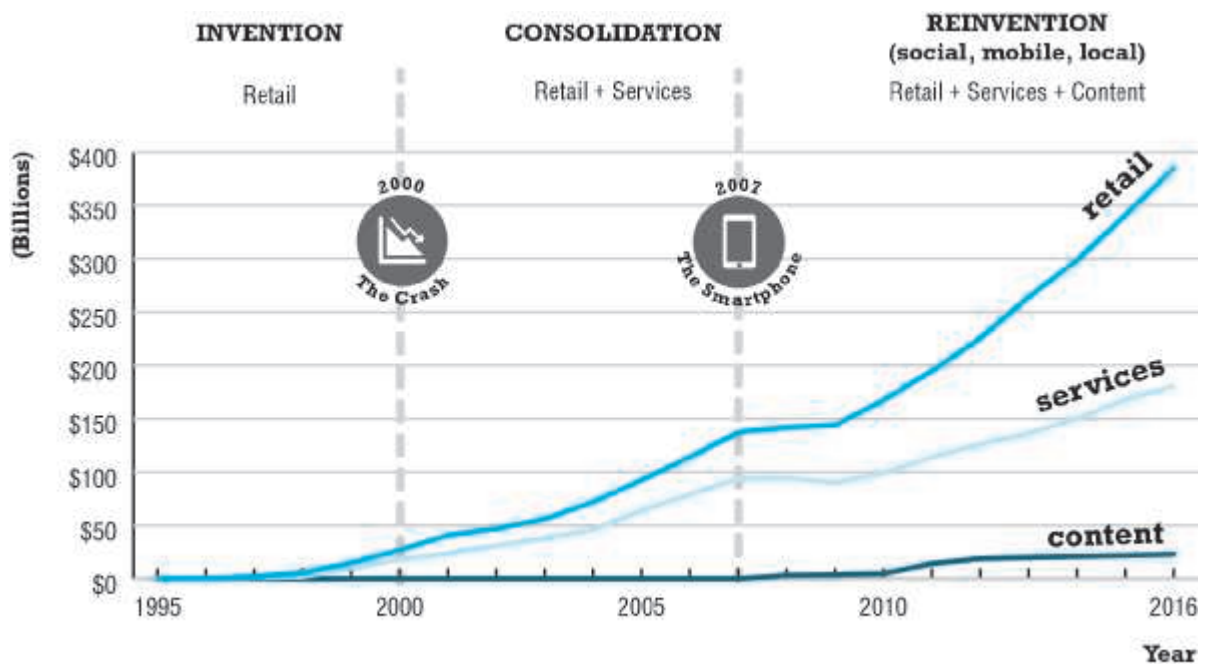
The early years of e-commerce were a period of explosive growth and extraordinary innovation. During this Invention period, e-commerce meant selling retail goods, usually quite simple goods, on the Internet. There simply was not enough bandwidth for more complex products. Marketing was limited to unsophisticated 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



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

direct access to hundreds of millions of customers. In this near-perfect information marketplace, 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).

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 marketplace 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 marketplace, 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

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

network effect

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

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 shrank 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

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

Web 2.0

set of applications and technologies that enable user-generated content

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	2001–2006	2007–PRESENT	
INVENTION	CONSOLIDATION	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 process (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.

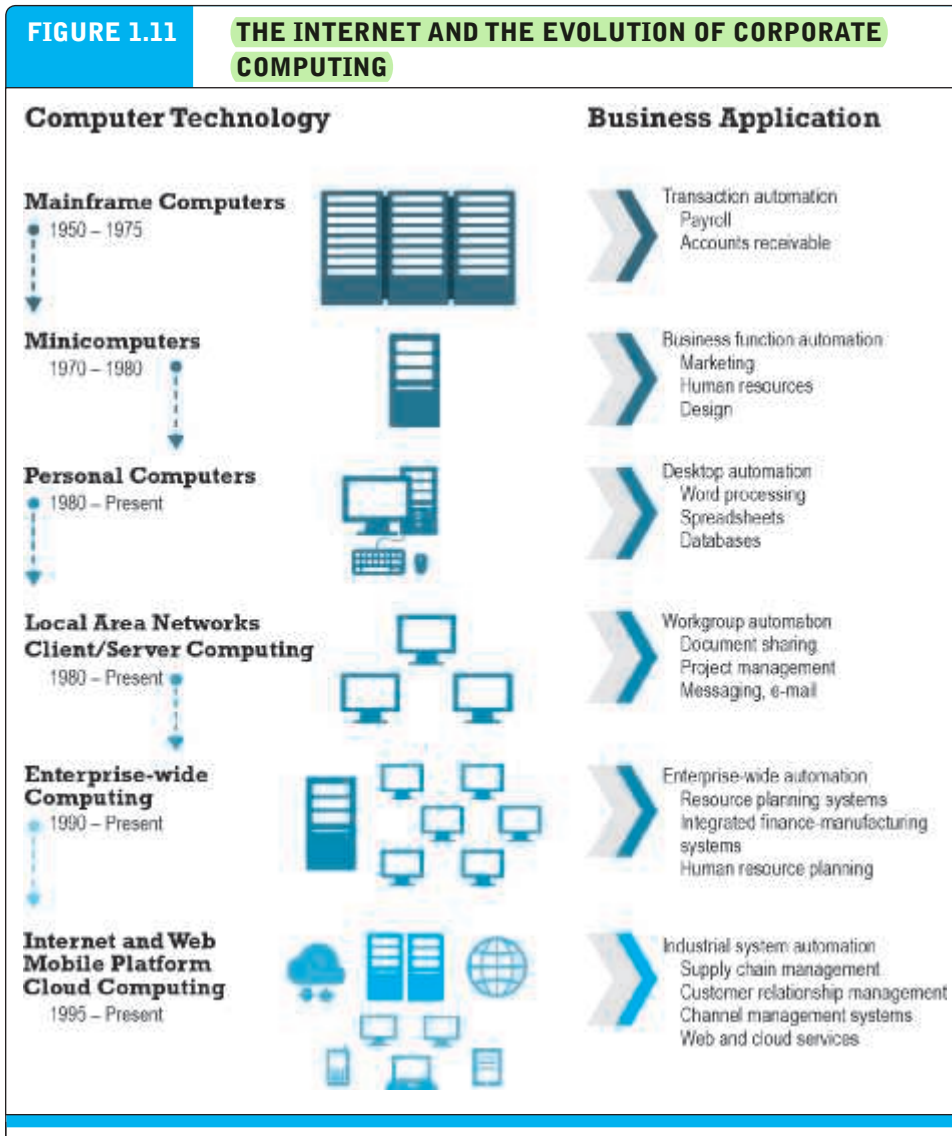
TECHNOLOGY: INFRASTRUCTURE

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.

BUSINESS: BASIC CONCEPTS

While technology provides the infrastructure, it is the business applications—the potential for extraordinary returns on investment—that create the interest and excitement in e-commerce. New technologies present businesses and entrepreneurs with new ways of organizing production and transacting business. New technologies change the strategies and plans of existing firms: old strategies are made obsolete and new ones need to be invented. New technologies are the birthing grounds where thousands of new companies spring up with new products and services. New technologies are the graveyard of many traditional businesses. To truly understand e-commerce, you will need to be familiar with some key business concepts, such as the nature of digital markets, digital goods, business models, firm and industry value chains, value webs, industry structure, digital disruption, and consumer behavior in digital markets, as well as basic concepts of financial analysis. We'll examine these concepts further in Chapters 2, 6, 7, and 9 through 12.

SOCIETY: TAMING THE JUGGERNAUT

With around 267 million Americans now using the Internet, many for e-commerce purposes, and more than 3.3 billion users worldwide, the impact of the Internet and e-commerce on society is significant and global. Increasingly, e-commerce is subject to the laws of nations and global entities. You will need to understand the pressures that global e-commerce places on contemporary society in order to conduct a successful e-commerce business or understand the e-commerce phenomenon. The primary societal issues we discuss in this book are individual privacy, intellectual property, and public welfare policy.

individual privacy

Because the Internet and the Web are exceptionally adept at tracking the identity and behavior of individuals online, e-commerce raises difficulties for preserving privacy—the ability of individuals to place limits on the type and amount of information collected about them, and to control the uses of their personal information. Read the *Insight on Society* case, *Facebook and the Age of Privacy*, to get a view of some of the ways e-commerce sites use personal information.

intellectual property rights

Because the cost of distributing digital copies of copyrighted intellectual property—tangible works of the mind such as music, books, and videos—is nearly zero on the Internet, e-commerce poses special challenges to the various methods societies have used in the past to protect intellectual property rights.

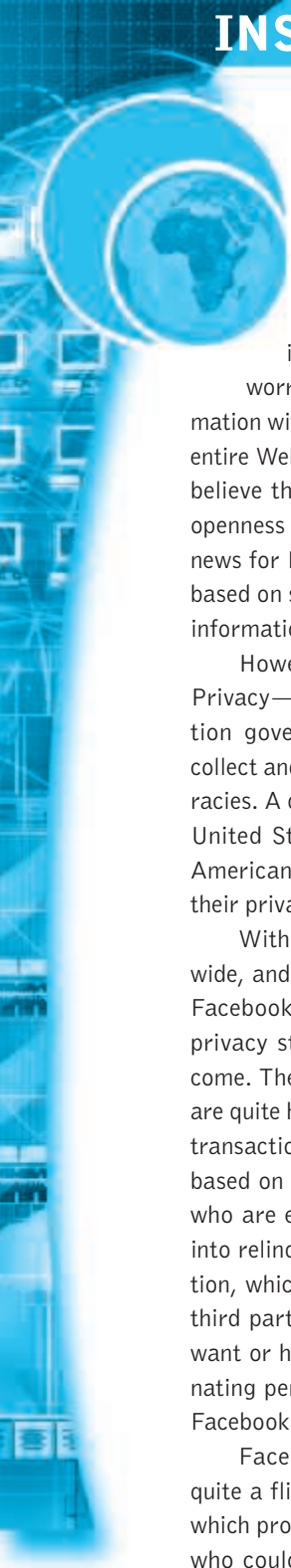
public welfare policy

The global nature of e-commerce also poses public policy issues of equity, equal access, content regulation, and taxation. For instance, in the United States, public telephone utilities are required under public utility and public accommodation laws to make basic service available at affordable rates so everyone can have telephone service. Should these laws be extended to the Internet and the Web? If goods are purchased by a New York State resident from a website in California, shipped from a center in Illinois, and delivered to New York, what state has the right to collect a sales tax? Should some heavy Internet users who consume extraordinary amounts of bandwidth by streaming endless movies be charged extra for service, or should the Internet be neutral with respect to usage? What rights do nation-states and their

Equity: giving what is needed to be successful

INSIGHT ON SOCIETY

FACEBOOK AND THE AGE OF PRIVACY



In a January 2010 interview, Mark Zuckerberg, the founder of Facebook, proclaimed that the age of privacy had to come to an end. According to Zuckerberg, people were no longer worried about sharing their personal information with friends, friends of friends, or even the entire Web. Supporters of Zuckerberg's viewpoint believe the twenty-first century is a new era of openness and transparency. If true, this is good news for Facebook because its business model is based on selling access to a database of personal information.

However, not everyone is a true believer. Privacy—limitations on what personal information government and private institutions can collect and use—is a founding principle of democracies. A decade's worth of privacy surveys in the United States show that well over 80% of the American public fear the Internet is a threat to their privacy.

With about 1.7 billion monthly users worldwide, and around 175 million in North America, Facebook's privacy policies are going to shape privacy standards on the Internet for years to come. The economic stakes in the privacy debate are quite high, involving billions in advertising and transaction dollars. Facebook's business model is based on building a database of billions of users who are encouraged, or even perhaps deceived, into relinquishing control over personal information, which is then sold to advertisers and other third parties. The less privacy Facebook's users want or have, the more Facebook profits. Eliminating personal information privacy is built into Facebook's DNA.

Facebook's current privacy policies are quite a flip-flop from its original policy in 2004, which promised users near complete control over who could see their personal profile. However,

every year since 2004, Facebook has attempted to extend its control over user information and content, often without notice. For instance, in 2007, Facebook introduced the Beacon program, which was designed to broadcast users' activities on participating websites to their friends. After a public outcry, Facebook terminated the Beacon program, and paid \$9.5 million to settle a host of class action lawsuits. In 2009, undeterred by the Beacon fiasco, Facebook unilaterally decided that it would publish users' basic personal information on the public Internet, and announced that whatever content users had contributed belonged to Facebook, and that its ownership of that information never terminated. However, as with the Beacon program, Facebook's efforts to take permanent control of user information resulted in users joining online resistance groups and it was ultimately forced to withdraw this policy as well.

In 2011, Facebook began publicizing users' "likes" of various advertisers in Sponsored Stories (i.e., advertisements) that included the users' names and profile pictures without their explicit consent, without paying them, and without giving them a way to opt out. This resulted in yet another class action lawsuit, which Facebook settled for \$20 million in June 2012. (Facebook dropped Sponsored Stories in April 2014.) In 2011, Facebook enrolled all Facebook subscribers into its facial recognition program without notice. This too raised the privacy alarm, forcing Facebook to make it easier for users to opt out.

In May 2012, Facebook went public, creating even more pressure to increase revenues and profits to justify its stock market value. Shortly thereafter, Facebook announced that it was launching a mobile advertising product that pushes ads to the mobile news feeds of users based on the apps they use through the Facebook Connect feature, without explicit permission from the user to do so. It also

(continued)

announced Facebook Exchange, a program that allows advertisers to serve ads to Facebook users based on their browsing activity while not on Facebook. Privacy advocates raised the alarm yet again and more lawsuits were filed by users. In 2013, Facebook agreed to partner with several data marketing companies that deliver targeted ads based on offline data. The firms provide customer data to Facebook, which then allows Facebook advertisers to target their ads to those users based on that data.

In December 2013, another class action lawsuit was filed against Facebook by users alleging that it violated their privacy by scanning users' private Facebook messages and mining them for data such as references to URLs that Facebook could then sell to advertisers. In May 2014, an enhancement to Facebook's mobile app that allows the app to recognize the music, television show, or movie playing in the background when a user makes a status update raised a new privacy alarm.

Facebook's newest privacy issue involves its facial recognition software used to tag users in photos. The "tag suggestions" feature is automatically enabled when you sign up, without user consent. A federal court in 2016 is allowing a lawsuit to go forward contesting Facebook's right to tag users in photos without their consent. This feature appears to be in violation of several state laws which seek to secure the privacy of biometric data.

After all these lawsuits and online public protests, one might think that Facebook's privacy

policy would improve. But an academic analysis of Facebook's privacy policies from 2008 to 2015 found that on most measures of privacy protection, Facebook's policies have worsened. Since 2008, Facebook has made it more difficult for users to find out what information is being shared with whom, how it builds profiles, or how to change privacy settings. Its privacy policies have become less readable, even inscrutable, according to the researchers.

Facebook is certainly aware of consumer suspicion of its privacy policies, and it changes its policies almost yearly in response to criticism. But the response is often not helpful for users, and typically extends the company's claims to do whatever it wants with personal information. Its latest privacy policy, implemented in 2015, claims to switch its default privacy settings for new users from Public to Friends, provide a Privacy Checkup tool for users, give users the ability to see the data it keeps on their likes and interests, and enable users to change, delete, or add to that data. Facebook argues this new policy gives users more control of the ads they are shown. Analysts point out, however, that using these new features requires users to navigate a maze of check boxes and menus that are difficult to understand even for expert Facebook users. Users have come to realize that everything they post or say on Facebook will be given over to advertisers. There is no privacy on Facebook. People who are concerned about their privacy, analysts have concluded, should delete their Facebook accounts.

— **SOURCES:** "Facebook's Newest Privacy Problem: 'Faceprint' Data" by Katie Collins, Cnet.com, May 16, 2016; "In Re Facebook Biometric Information Privacy Litigation," U.S. District Court, Northern District of California, Case No. 15-cv-03747-JD, May 6, 2016; "Facebook to Face Privacy Lawsuit Over Photo Tagging," by Jessica Guynn, *USA Today*, May 6, 2016; "Facebook Rescinds Internship to Harvard Student Who Exposed a Privacy Flaw in Messenger," by Robert Gabelhoff, *Washington Post*, August 14, 2015; "Did You Really Agree to That? The Evolution of Facebook's Privacy Policy," by Jennifer Shore and Jill Steinman, *Technology Science*, August 11, 2015; "Facebook's Privacy Incident Response: A Study of Geolocation Sharing on Facebook Messenger," by Aran Khanna, *Technology Science*, August 11, 2015; "Sharing Data, but Not Happily," by Natasha Singer, *New York Times*, June 4, 2015; "How Your Facebook Likes Could Cost You a Job," by Anna North, *New York Times*, January 20, 2015; "Facebook Stops Irresponsibly Defaulting Privacy of New Users' Posts to 'Public,' Changes to 'Friends,'" by Josh Constine, Techcrunch.com, May 22, 2014; "Facebook Users Revolt Over Privacy Feature—Enables Microphone in Apps," by Jan Willem Aldershoff, Myce.com, June 9, 2014; "Didn't Read Those Terms of Service? Here's What You Agreed to Give Up," by Natasha Singer, *New York Times*, April 28, 2014; "Facebook Eliminates Sponsored Stories—Will It Matter to Advertisers?," by Amy Durbin, Mediapost.com, February 25, 2014; "Facebook Sued for Allegedly Intercepting Private Messages," by Jennifer Van Grove, Cnet.com, January 2, 2014; "Facebook to Partner with Data Brokers," by Bob Sullivan, Redtape.nbcnews.com, February 26, 2013; "Facebook Exchange Ads Raise Privacy Concerns," by Mikal E. Belicove, Cnbc.com, June 21, 2012; "Facebook Suit Over Subscriber Tracking Seeks \$15 Billion," by Kit Chellel and Jeremy Hodges, Bloomberg.com, May 19, 2012; "How Facebook Pulled a Privacy Bait and Switch," by Dan Tynan, *PC World*, May 2010.

citizens have with respect to the Internet, the Web, and e-commerce? We address issues such as these in Chapter 8, and also throughout the text.

1.7 ACADEMIC DISCIPLINES CONCERNED WITH E-COMMERCE

The phenomenon of e-commerce is so broad that a multidisciplinary perspective is required. There are two primary approaches to e-commerce: technical and behavioral.

TECHNICAL APPROACHES

Computer scientists are interested in e-commerce as an exemplary application of Internet technology. They are concerned with the development of computer hardware, software, and telecommunications systems, as well as standards, encryption, and database design and operation. Operations management scientists are primarily interested in building mathematical models of business processes and optimizing these processes. They are interested in e-commerce as an opportunity to study how business firms can exploit the Internet to achieve more efficient business operations. The information systems discipline spans the technical and behavioral approaches. Technical groups within the information systems specialty focus on data mining, search engine design, and artificial intelligence.

BEHAVIORAL APPROACHES

From a behavioral perspective, information systems researchers are primarily interested in e-commerce because of its implications for firm and industry value chains, industry structure, and corporate strategy. Economists have focused on online consumer behavior, pricing of digital goods, and on the unique features of digital electronic markets. The marketing profession is interested in marketing, brand development and extension, online consumer behavior, and the ability of e-commerce technologies to segment and target consumer groups, and differentiate products. Economists share an interest with marketing scholars who have focused on e-commerce consumer response to marketing and advertising campaigns, and the ability of firms to brand, segment markets, target audiences, and position products to achieve above-normal returns on investment.

Management scholars have focused on entrepreneurial behavior and the challenges faced by young firms who are required to develop organizational structures in short time spans. Finance and accounting scholars have focused on e-commerce firm valuation and accounting practices. Sociologists—and to a lesser extent, psychologists—have focused on general population studies of Internet usage, the role of social inequality in skewing Internet benefits, and the use of the Web as a social network and group communications tool. Legal scholars are interested in issues such as preserving intellectual property, privacy, and content regulation.

No one perspective dominates research about e-commerce. The challenge is to learn enough about a variety of academic disciplines so that you can grasp the significance of e-commerce in its entirety.

1.8

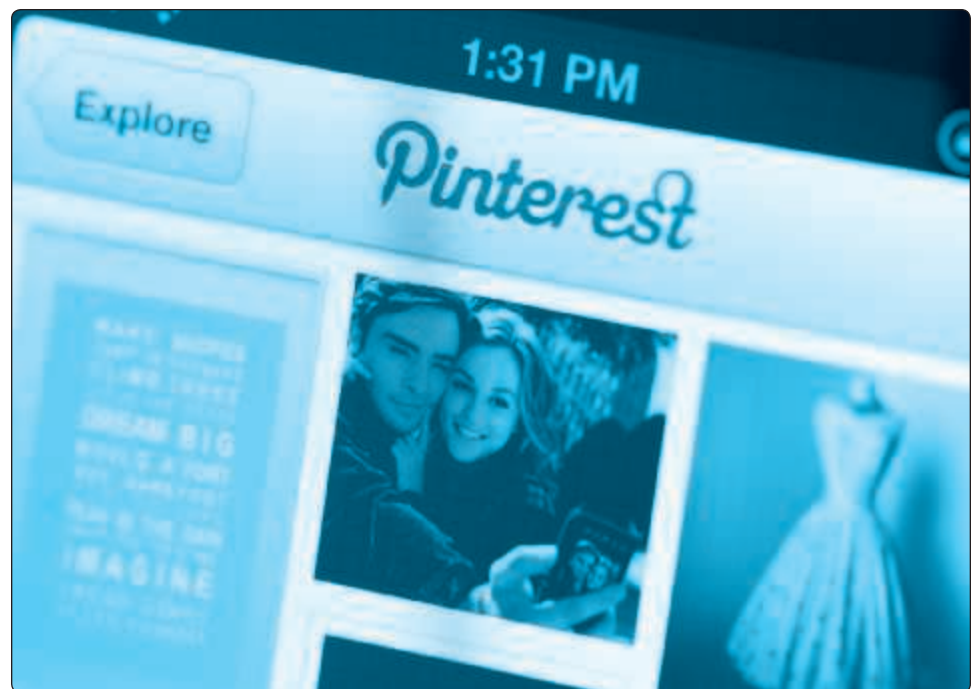
CASE STUDY

P i n t e r e s t :

A Picture Is Worth a Thousand Words

Like all successful e-commerce companies, Pinterest taps into a simple truth. In Pinterest's case, the simple truth is that people love to collect things, and show off their collections to others. Founded in 2009 by Ben Silbermann, Evan Sharp, and Paul Sciarra and launched in March 2010, Pinterest allows you to create virtual scrapbooks of images, video, and other content that you "pin" (save) to a virtual bulletin board or pin board. Categories range from Animals to Videos, with Food & Drink, DIY & Crafts, Home Décor, and Women's Fashion among the most popular. Find something that you particularly like? In addition to "liking" and perhaps commenting on it, you can re-pin it to your own board or follow a link back to the original source. Find someone whose taste you admire or who shares your passions? You can follow one or more of that pinner's boards to keep track of everything she or he pins. As of October 2016, there were over 50 billion pins on Pinterest on more than 1 billion different boards.

Pinterest originally positioned itself as a social network. However, it has changed its tune and now describes itself as a visual search tool for discovering and saving creative



ideas (and potential purchases), with less emphasis on sharing with friends. Search has become the core part of its mission. It views Google, rather than Facebook, Twitter, or Instagram, as its primary competition.

In October 2016, Pinterest has over 150 million monthly active members worldwide. About 75% of those members are women, but men are its fastest growing demographic. Pinterest is one of the “stickiest” sites on the Web, with women spending over 1.5 hours (96 minutes) per session, and men about 1.25 hours (75 minutes). According to a survey by the Pew Research Center, the percentage of online adults in the United States who use Pinterest has more than doubled since 2012.

Over the past five years, investors such as well-known Silicon Valley venture capital firms Andreessen Horowitz and Bessemer Venture Partners, hedge fund Valiant Capital Partners, and Japanese e-commerce company Rakuten have poured over \$1.3 billion in venture capital into Pinterest, with its latest round of funding in May 2015 valuing the company at \$11 billion, more than double its 2014 valuation. Like Facebook, Twitter, and many other startup companies, Pinterest focused initially on refining its product and building its user base, but not surprisingly, its investors began to push it to begin generating revenue. Pinterest’s first step was to offer business accounts that provided additional resources for brands. In 2013, it introduced Rich Pins, which allowed companies to embed information, such as current pricing and availability, as well as a direct link to a product page. In 2014, Pinterest took the official leap into the advertising arena, launching a beta version of ads it called Promoted Pins that appear in search results and category feeds. Around the same time, Pinterest also introduced a search engine, called Guided Search, which suggests related terms to refine a search. Guided Search is based on user metadata, such as board titles, captions, and comments related to pins, to create different categories and subcategories. In January 2015, Pinterest further enhanced Guided Search by allowing users to personalize search results based on gender.

In the last two years, Pinterest has gotten serious about monetization. In January 2015, it rolled out Promoted Pins to all its U.S.-based partners and in April 2016, began offering them to advertisers in the United Kingdom, with additional English-speaking countries expected to be added later in the year. In May 2015, it added Cinematic Pins, a made-for-mobile format. Cinematic Pins display a short animation when the user scrolls down through the ad, and only play a full-length version when the user clicks on the ad, providing more user control over the experience. Pinterest also introduced new ad-targeting and pricing options. Advertisers can target users by interests, life stage, or “persona” such as Millennial, prospective parent, or foodie. In June 2016, it added three additional ad-targeting options: custom list targeting (similar to Facebook’s Custom Audiences); visitor targeting, which allows advertisers to retarget a customer who has visited the advertiser’s website; and lookalike targeting, which enables advertisers to target consumers who share traits or behaviors with the advertiser’s existing customers. Ads can be purchased on a pay-per-view, pay-per-click, cost-per-engagement (CPE), or cost-per-action (CPA) model. Using the CPE model, advertisers only pay when a user engages with a pin, such as through re-pinning, and with the CPA model, only when the user clicks through to a website and makes a purchase or downloads an app. As of 2016, there are more than 1 million businesses on Pinterest, and over 10,000 different advertisers. During 2016,

SOURCES: “As Pinterest Hits 150MM Actives, It’s Time to Re-Think Your Social Approach,” by Allie Wassum, *Huffingtonpost.com*, October 17, 2016; “Pinterest Starts Expanding Its Visual Search Tools to Video,” by Matthew Lynley, *Techcrunch.com*, August 4, 2016; “Social’s Next Evolution? Pinterest Begins to Monetize Users’ Search,” *eMarketer, Inc.*, July 15, 2016; “Amid IPO Speculation, Pinterest Hangs a Target on Alphabet’s Back,” by John-Erik Koslosky, *Fool.com*, July 11, 2016; “Pinterest Adds Features as It Looks to Monetize 55 Million Active Users,” by Emily Rolen, *Thestreet.com*, July 6, 2016; “Pinterest Updates Strategy, Looks to Scale Search and Audience Based Buying,” by

George Siefko, Adage.com, July 5, 2016; "Pinterest Doubles Down on the Shopping Cart Wars," by Thom Forbes, Mediapost.com, June 29, 2016; "Pinterest Hopes to Woo Shoppers with Visual Search," by Rachel Metz, *MIT Technology Review*, June 28, 2016; "Pinterest Makes a Major E-commerce Push," by Zak Stambor, Internetretailer.com, June 28, 2016; "Pinterest Ramps Up Its Ad Targeting Options," by Zak Stambor, Internetretailer.com, June 14, 2016; "Pinterest Renames 'Pin It' Button as 'Save' in Push for Global Growth," by Kathleen Chaykowski, Forbes.com, June 2, 2016; "Pinterest Broadens Ad Sales Focus Once Again," by Jack Marshall, *Wall Street Journal*, May 2, 2016; "Pinterest's Plans for World Domination," by Lara O'Reilly, Businessinsider.com, April 28, 2016; "Pinterest Is a Sleeping Giant – Don't Underestimate It," by Madjumita Murgia, Telegraph.co.uk, April 28, 2016; "Pinterest Announces Complete Overhaul of iOS App with Performance & Visual Improvements," by Chance Miller, 9to5mac.com, April 19, 2016; "Pinterest Launches Promoted Pins Internationally, Starting with the U.K.," by Paul Sawers, Venturebeat.com, April 7, 2016; "Final Update on Boffoli Case Against Pinterest," *Ipforthelittleguy.com*, March 26, 2016; "Pinterest Sharpens Its Visual Search Skills," by Yoree Koh, *Wall Street Journal*, November 8, 2015; "Mobile Messaging and Social Media 2015," by Maeve Duggan, Pewinternet.org, August 19, 2015; "In Lawsuit Against Pinterest, Artist Continues a Crusade for Copyright on the Internet," by Kate Lucas, Grossmanllp.com, July 23, 2015; "With Buyable Pins, Pinterest Lets You Buy Stuff Right in the App," by JP Mangalindan, Mashable.com, June 2, 2015; "Why \$11 Billion Pinterest Thinks It Has the 'Best Kind of Business Model'," by Jillian D'Onfrio, Businessinsider.com, May 19, 2015; "Pinterest Doubles Down on Making Money, Rolls Out Video Ads," by JP Mangalindan, Mashable.com, May 19, 2015; "Pinterest Puts Its Own Spin on Video Ads with These Cinematic Pins," by Garret Sloane, Adweek.com, May 19, 2015; "How Pinterest Plans to Spend Its New

Pinterest plans to broaden its focus from retail and packaged goods to financial services, travel, automotive, and fast food restaurants.

Search advertising is the next frontier for Pinterest. Pinterest search differs from other types of search because it is visual and typically happens at the early stages of a person's decision process. Users currently conduct over 2 billion keyword and 130 million visual searches per month on Pinterest. In July 2016, Pinterest began offering its search inventory to advertisers for the first time and is reportedly working on the infrastructure for keyword-based buying. Pinterest believes search advertising revenue can become a significant part of its business, and that it can challenge Google in the mobile search arena. It is making significant investments in search technology, such as deep-learning assisted visual search, which will build on its existing visual search tool that allows users to search within images on Pinterest. In August 2016, it began updating its visual search tools to work on videos and also began rolling out a fully integrated native video player similar to that offered by Facebook, along with video ads.

Many analysts also believe that Pinterest will become a significant factor in the social e-commerce arena. In June 2015, Pinterest launched Buyable Pins, which allow users to directly purchase products by clicking a blue Buy It button within the pin, for its iPhone and iPad apps. Buyable Pins for Android devices were rolled out in November 2015, and in June 2016 finally reached the desktop. According to Pinterest, 10 million unique items are available for sale, from merchants both large (such as Macy's, Nordstrom, Neiman Marcus, Bloomingdale's, and Wayfair) and small. Pinterest says its data shows that Buyable Pins are generating a significant percentage of brand-new customers for merchants. Pinterest is significantly ahead of other social networks such as Facebook, Instagram, and Twitter in terms of the percentage of users who use it to find or shop for products: 55% for Pinterest versus just 12% for Facebook and Instagram and 9% for Twitter. To further enhance its lead, in 2016, it announced a number of other e-commerce-related initiatives, including Shopping with Pinterest, a shopping cart that links to a user's account, is visible on all devices, can hold multiple items, and allows for checkout on any device.

The fact that Pinterest launched Buyable Pins on its iOS mobile platform rather than the desktop is just one indication of how important the mobile platform is to Pinterest. Pinterest provides apps for iPhone, iPad, Android, and Windows Phone, as well as a mobile version of its website using HTML5. Pinterest Mobile runs inside the smartphone's browser rather than as a stand-alone program. Mobile has been a huge success for Pinterest, with 80% of its traffic coming from mobile devices in 2016. Pinterest releases new versions of its mobile apps on a regular basis, and in April 2016 launched a nearly completely written iOS app that allows the home page to load much more quickly, scales to the different number of iOS screens more efficiently, and is readable in all 31 languages in which Pinterest is available. According to Pinterest co-founder Evan Sharp, the smartphone is the platform Pinterest focuses on when it develops new features and products.

International expansion continues to be a major area of focus. Pinterest introduced its first localized site, for the United Kingdom in May 2013, and it is now available in 31 different languages. Pinterest is aiming to make its platform feel more regional, focusing specifically on the United Kingdom, France, Germany, Japan, and Brazil. In 2016, for the first time, more than 50% of its monthly active users are located outside of the United

States. Looking to the future, Pinterest believes that international expansion will provide it with the greatest growth opportunities.

Despite all the good news for Pinterest, there are some issues lurking just behind the scenes that may cloud its future, such as the issue of copyright infringement. The basis of Pinterest's business model involves users potentially violating others' copyrights by posting images without permission and/or attribution. Although Pinterest's Terms of Service puts the onus on its users to avoid doing so, the site knowingly facilitates such actions by, for example, providing a Pin It tool embedded in the user's browser toolbar. Much content on the site reportedly violates its Terms of Service. Pinterest has provided an opt-out code to enable other sites to bar its content from being shared on Pinterest, but some question why they should have to take action when Pinterest is creating the problem. Another thing Pinterest has done to try to ameliorate the problem is to automatically add citations (attribution) to content coming from certain specified sources, such as Flickr, YouTube, Vimeo, Etsy, Kickstarter, and SlideShare, among others. In 2013, it entered into an agreement with Getty Images in which it agreed to provide attribution for Getty content and pay Getty a fee. Pinterest says it complies with the Digital Millennium Copyright Act, which requires sites to remove images that violate copyright, but this too requires the copyright holder to be proactive and take action to demand the images be removed. Christopher Boffoli, a well-known photographer, filed a federal lawsuit against Pinterest in late 2014 alleging that Pinterest users used his photographs without his permission and that Pinterest failed to take adequate measures to remove them. In September 2015, Boffoli agreed to dismiss the case, presumably as part of a confidential settlement with Pinterest, leaving the legal issues raised unresolved.

Pinterest is also not immune to the spam and scams that plague many e-commerce initiatives. Security analysts believe Pinterest will have to adapt its systems to deal with scammers and warn users to be wary of requests to pin content before viewing it and to be suspicious of "free" offers, surveys, and links with questionable titles. Pinterest has acknowledged the problem and has promised to improve its technology. In 2015, for instance, Pinterest migrated its website to the HTTPS protocol, which provides more security than the more common HTTP protocol typically used to access web pages. Pinterest also employs a system known as Stingray that enables it to quickly react to spam and other types of malicious behavior, and has created a program that pays a bounty to white hat hackers who discover security issues.

At the moment, however, the future looks very bright for Pinterest as it reportedly gears up for an initial public offering in the near future. Although it may encounter some growing pains in the process of implementing its new business model, it has the potential to generate significant revenue based on advertising and social e-commerce.

Millions and Why It Only Hires Nice Employees, According to Its Cofounder," by Jillian D'Onfrio, *Businessinsider.com*, May 11, 2015; "Pinterest Beefs Up Security with Full HTTPS Support and Bug Bounty Program," by Jordan Novet, *Venturebeat.com*, March 13, 2015; "Fighting Spam at Pinterest," *Engineering.pinterest.com*, February 20, 2015; "Pinterest Goes After the Male Demographic with Debut of New Search Filters," by Sarah Perez, *Techcrunch.com*, January 23, 2015; "Pinterest Becomes More Search Engine-Like with the Launch of Guided Search on the Web," by Sarah Perez, *Techcrunch.com*, June 11, 2014; "Pinterest Tests Do-It-Yourself Promoted Pins for Small and Medium-Sized Businesses," by Ryan Lawler, *Techcrunch.com*, June 5, 2014; "Can Pinterest Be Found in Translation," by Sarah Frier, *Businessweek.com*, May 22, 2014; "Pinterest's Next Big Move: A Clever New Take on Search," by Kyle VanHemert, *Wired.com*, April 24, 2014; "Paying for Pin-Ups," by Sarah Laskow, *Columbia Journalism Review*, November 7, 2013; "Pinning Down Pinterest: Addressing Copyright and Other IP Issues," by Jennifer L. Barry, *Lexology.com*, October 22, 2013; "Pinterest (Officially) Jumps the Pond," by Zak Stambor, *Internetretailer.com*, May 10, 2013; "Pinterest Gives Copyright Credit to Etsy, Kickstarter, SoundCloud," by Sarah Kessler, *Mashable.com*, July 19, 2012; "A Site That Aims to Unleash the Scrapbook Maker in All of Us," by Jenna Wortham, *New York Times*, March 11, 2012; "Pinterest Releases Optional Code to Prevent Unwanted Image Sharing," by Andrew Webster, *Theverge.com*, February 20, 2012; "A Scrapbook on the Web Catches Fire," by David Pogue, *New York Times*, February 15, 2012.

Case Study Questions

1. Why does Pinterest view Google as its primary competitor?
2. Why does Pinterest focus on the smartphone platform when it develops new features and products?
3. Why is copyright infringement a potential issue for Pinterest?

1.9 REVIEW

KEY CONCEPTS

- Understand why it is important to study e-commerce.
 - The next five years hold out exciting opportunities—as well as risks—for new and traditional businesses to exploit digital technology for market advantage. It is important to study e-commerce in order to be able to perceive and understand these opportunities and risks that lie ahead.
- Define e-commerce, understand how e-commerce differs from e-business, identify the primary technological building blocks underlying e-commerce, and recognize major current themes in e-commerce.
 - E-commerce involves digitally enabled commercial transactions between and among organizations and individuals.
 - E-business refers primarily to the digital enabling of transactions and processes within a firm, involving information systems under the control of the firm. For the most part, unlike e-commerce, e-business does not involve commercial transactions across organizational boundaries where value is exchanged.
 - The technology juggernauts behind e-commerce are the Internet, the Web, and increasingly, the mobile platform.
 - From a business perspective, one of the most important trends to note is that all forms of e-commerce continue to show very strong growth. From a technology perspective, the mobile platform has finally arrived with a bang, driving astronomical growth in mobile advertising and making true mobile e-commerce a reality. At a societal level, major issues include privacy and government surveillance, protection of intellectual property, online security, and governance of the Internet.
- Identify and describe the unique features of e-commerce technology and discuss their business significance.

There are eight features of e-commerce technology that are unique to this medium:

- *Ubiquity*—available just about everywhere, at all times, making it possible to shop from your desktop, at home, at work, or even from your car.
- *Global reach*—permits commercial transactions to cross cultural and national boundaries far more conveniently and cost-effectively than is true in traditional commerce.
- *Universal standards*—shared by all nations around the world, in contrast to most traditional commerce technologies, which differ from one nation to the next.
- *Richness*—enables an online merchant to deliver marketing messages in a way not possible with traditional commerce technologies.
- *Interactivity*—allows for two-way communication between merchant and consumer and enables the merchant to engage a consumer in ways similar to a face-to-face experience, but on a much more massive, global scale.
- *Information density*—is the total amount and quality of information available to all market participants. The Internet reduces information collection, storage, processing, and communication costs while increasing the currency, accuracy, and timeliness of information.
- *Personalization and customization*—the increase in information density allows merchants to target their marketing messages to specific individuals and results in a level of personalization and customization unthinkable with previously existing commerce technologies.
- *Social technology*—provides a many-to-many model of mass communications. Millions of users are able to generate content consumed by millions of other users. The result is the formation of social networks on a wide scale and the aggregation of large audiences on social network platforms.

■ Describe the major types of e-commerce.

There are six major types of e-commerce:

- *B2C e-commerce* involves businesses selling to consumers and is the type of e-commerce that most consumers are likely to encounter.
- *B2B e-commerce* involves businesses selling to other businesses and is the largest form of e-commerce.
- *C2C e-commerce* is a means for consumers to sell to each other. 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.
- *Social e-commerce* is e-commerce that is enabled by social networks and online social relationships.
- *M-commerce* involves the use of wireless digital devices to enable online transactions.
- *Local e-commerce* is a form of e-commerce that is focused on engaging the consumer based on his or her current geographic location.

■ Understand the evolution of e-commerce from its early years to today.

E-commerce has gone through three stages: innovation, consolidation, and reinvention.

- The early years of e-commerce were a technological success, with the digital infrastructure created during the period solid enough to sustain significant growth in e-commerce during the next decade, and a mixed business success, with significant revenue growth and customer usage, but low profit margins.
- E-commerce entered a period of consolidation beginning in 2001 and extending into 2006.
- E-commerce entered a period of reinvention in 2007 with the emergence of the mobile digital platform, social networks, and Web 2.0 applications that attracted huge audiences in a very short time span.

■ Describe the major themes underlying the study of e-commerce.

E-commerce involves three broad interrelated themes:

- *Technology*—To understand e-commerce, you need a basic understanding of the information technologies upon which it is built, including the Internet, the Web, and mobile platform, and a host of complementary technologies—cloud computing, desktop computers, smartphones, tablet computers, local area networks, client/server computing, packet-switched communications, protocols such as TCP/IP, web servers, HTML, and relational and non-relational databases, among others.
- *Business*—While technology provides the infrastructure, it is the business applications—the potential for extraordinary returns on investment—that create the interest and excitement in e-commerce. Therefore, you also need to understand some key business concepts such as electronic markets, information goods, business models, firm and industry value chains, industry structure, and consumer behavior in digital markets.
- *Society*—Understanding the pressures that global e-commerce places on contemporary society is critical to being successful in the e-commerce marketplace. The primary societal issues are intellectual property, individual privacy, and public policy.

■ Identify the major academic disciplines contributing to e-commerce.

There are two primary approaches to e-commerce: technical and behavioral. Each of these approaches is represented by several academic disciplines.

- On the technical side, this includes computer science, operations management, and information systems.
- On the behavioral side, it includes information systems as well as sociology, economics, finance and accounting, management, and marketing.

QUESTIONS

1. What is e-commerce? How does it differ from e-business? Where does it intersect with e-business?
2. What is information asymmetry?
3. What are some of the unique features of e-commerce technology?
4. What is a marketplace?
5. What are three benefits of universal standards?
6. Compare online and traditional transactions in terms of richness.
7. **Name three of the business** consequences that can result from growth in information density.
8. What is Web 2.0? Give examples of Web 2.0 sites and explain why you included them in your list.
9. Give examples of B2C, B2B, C2C, and social, mobile, and local e-commerce besides those listed in the chapter materials.
10. How are e-commerce technologies similar to or different from other technologies that have changed commerce in the past?
11. Describe the three different stages in the evolution of e-commerce.
12. Define disintermediation and explain the benefits to Internet users of such a phenomenon. How does disintermediation impact friction-free commerce?
13. What are some of the major advantages and disadvantages of being a first mover?
14. What is a network effect, and why is it valuable?
15. Discuss the ways in which the early years of e-commerce can be considered both a success and a failure.
16. What are five of the major differences between the early years of e-commerce and today's e-commerce?
17. Why is a multidisciplinary approach necessary if one hopes to understand e-commerce?
18. What are some of the privacy issues that Facebook has created?
19. What are those who take a behavioral approach to studying e-commerce interested in?

PROJECTS

1. Choose an e-commerce company and assess it in terms of the eight unique features of e-commerce technology described in Table 1.2. Which of the features does the company implement well, and which features poorly, in your opinion? Prepare a short memo to the president of the company you have chosen detailing your findings and any suggestions for improvement you may have.
2. Search the Web for an example of each of the major types of e-commerce described in Section 1.4 and listed in Table 1.3. Create a presentation or written report describing each company (take a screenshot of each, if possible), and explain why it fits into the category of e-commerce to which you have assigned it.
3. Given the development and history of e-commerce in the years from 1995–2016, what do you predict we will see during the next five years of e-commerce? Describe some of the technological, business, and societal shifts that may occur as the Internet continues to grow and expand. Prepare a brief presentation or written report to explain your vision of what e-commerce will look like in 2020.
4. Prepare a brief report or presentation on how companies are using Instagram or another company of your choosing as a social e-commerce platform.
5. Follow up on events at Uber since October 2016 (when the opening case was prepared). Prepare a short report on your findings.

REFERENCES

- Bakos, Yannis. "Reducing Buyer Search Costs: Implications for Electronic Marketplaces." *Management Science* (December 1997).
- Banerjee, Suman, and Chakravarty, Amiya. "Price Setting and Price Discovery Strategies with a Mix of Frequent and Infrequent Internet Users." (April 15, 2005). SSRN: <http://ssrn.com/abstract=650706>.
- Camhi, Jonathan. "BI Intelligence Projects 34 Billion Devices Will Be Connected by 2020." *Businessinsider.com* (November 6, 2015).
- Cavallo, Alberto F. "Are Online and Offline Prices Similar? Evidence from Large Multi-Channel Retailers." NBER Working Paper No. 22142. (March 2016).
- eBay, Inc. "Form 10-K for the fiscal year ended December 31, 2015." (February 1, 2016).
- eMarketer, Inc. "US Internet Users and Penetration, 2015–2020." (August 3, 2016a).
- eMarketer, Inc. "US Mobile Connections, 2014–2020." (February 2016b).
- eMarketer, Inc. "US Internet Users, by Device, 2015–2020." (August 2, 2016c).
- eMarketer, Inc. "Internet Users and Penetration Worldwide, 2015–2020." (September 1, 2016d).
- eMarketer, Inc. "US Retail Ecommerce Sales, 2014–2020." (September 1, 2016e).
- eMarketer, Inc. "US Digital Travel Sales, 2014–2020." (April 26, 2016f).
- eMarketer, Inc. "US Retail Mcommerce Sales, 2014–2016." (September 1, 2016g.)
- eMarketer, Inc. "US Mobile Travel Sales, 2014–2020." (April 26, 2016h).
- eMarketer, Inc. "US Retail Mcommerce Sales, 2013–2019." (May 2015a)
- eMarketer, Inc. "US Mobile Travel Sales, 2013–2019." (May 1, 2015b).
- eMarketer, Inc. "US B2C Mcommerce Sales, 2012–2018." (April 2014).
- Evans, Philip, and Thomas S. Wurster. "Getting Real About Virtual Commerce." *Harvard Business Review* (November–December 1999).
- Evans, Philip, and Thomas S. Wurster. "Strategy and the New Economics of Information." *Harvard Business Review* (September–October 1997).
- Forrester Research. "U.S. Cross-Channel Retail Forecast, 2015 to 2020." (January 26, 2016).
- Ghose, Anindya, and Yuliang Yao. "Using Transaction Prices to Re-Examine Price Dispersion in Electronic Markets." *Information Systems Research*, Vol. 22 No. 2. (June 2011).
- Gorodnichenko, Yuriy, et al. "Price Setting in Online Markets: Does IT Click?" NBER Working Paper No. 20819 (December 2014).
- Interactions Consumer Experience Marketing, Inc., "The Rise of Webrooming." (May 2014).
- Internet Retailer. "Top 500 Guide 2016 Edition." (2016).
- Internet Systems Consortium, Inc. "ISC Internet Domain Survey." (January 2016).
- Kalakota, Ravi, and Marcia Robinson. *e-Business 2.0: Roadmap for Success, 2nd edition*. Reading, MA: Addison Wesley (2003).
- Kambil, Ajit. "Doing Business in the Wired World." *IEEE Computer* (May 1997).
- Levin, Jonathon. "The Economics of Internet Markets." NBER Working Paper No 16852 (February 2011).
- Mesenbourg, Thomas L. "Measuring Electronic Business: Definitions, Underlying Concepts, and Measurement Plans." U. S. Department of Commerce Bureau of the Census (August 2001).
- Rayport, Jeffrey F., and Bernard J. Jaworski. *Introduction to E-commerce, 2nd edition*. New York: McGraw-Hill (2003).
- Rosso, Mark, and Bernard Jansen. "Smart Marketing or Bait & Switch: Competitors' Brands as Keywords in Online Advertising." Proceedings of the 4th Workshop on Information Credibility. ACM (2010).
- Schwartz, Barry. "Google: We Know About 30 Thousand Trillion URLs on the Web, But..." *Seroundtable.com* (June 3, 2015).
- Shapiro, Carl, and Hal R. Varian. *Information Rules. A Strategic Guide to the Network Economy*. Cambridge, MA: Harvard Business School Press (1999).
- Sinha, Indrajit. "Cost Transparency: The Net's Threat to Prices and Brands." *Harvard Business Review* (March–April 2000).
- Smith, Michael, Joseph Bailey, and Erik Brynjolfsson. "Understanding Digital Markets: Review and Assessment." In Erik Brynjolfsson and Brian Kahin (eds.), *Understanding the Digital Economy*. Cambridge, MA: MIT Press (2000).
- Tversky, A., and D. Kahneman. "The Framing of Decisions and the Psychology of Choice." *Science* (January 1981).
- U.S. Census Bureau. "E-Stats." (June 7, 2016).
- Varian, Hal R. "When Commerce Moves On, Competition Can Work in Strange Ways." *New York Times* (August 24, 2000a).
- Varian, Hal R. "5 Habits of Highly Effective Revolution." *Forbes ASAP* (February 21, 2000b).



CHAPTER

2

E-commerce Business Models and Concepts

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Identify the key components of e-commerce business models.
- Describe the major B2C business models.
- Describe the major B2B business models.
- Understand key business concepts and strategies applicable to e-commerce.

Tweet Tweet:

Twitter's Business Model

Twitter, the social network based on 140-character text messages, continues in the long tradition of Internet developments that emerged seemingly out of nowhere to take the world by storm. Twitter's basic idea was to marry short text messaging on cell phones with the Web and its ability to create social groups.

Twitter has since expanded beyond simple text messages to article previews, photographs, videos, and even animated images, and today has over 310 million active users worldwide (as of June 2016). The 5,000 tweets a day that it began with in 2006 has turned into a deluge of around 6,000 tweets per second and 500 million per day worldwide. Special events, such as the Super Bowl, tend to generate an explosion of tweets, with a total of 28.4 million tweets during the course of the game in 2015. Some celebrities, such as the pop star Katy Perry, have millions of followers (in Perry's case, over 90 million as of 2016).

Like many social network firms, Twitter began operating without any revenue stream. However, it quickly developed some important assets, such as user attention and audience size (unique visitors). Another important asset is its database of tweets, which contain the real-time comments, observations, and opinions of its audience, and a search engine that can mine those tweets for patterns. In addition, Twitter has become a powerful alternative media platform for the distribution of news, videos, and pictures. Twitter has sought to monetize its platform via three primary advertising options, Promoted Tweets, Promoted Trends, and Promoted Accounts, although it continues to develop more and more variations on these products.

Promoted Tweets are Twitter's version of Google's search ads. In response to a search on Twitter for tablet computers, for example, a Best Buy Promoted Tweet about tablets might be displayed. Promoted Tweets typically cost between 20 cents and \$10. Twitter also offers geo-targeted and keyword targeting functionality, which enables advertisers to send Promoted Tweets to specific users in specific locations or based on their Twitter activity. Twitter's research indicates that users are much more likely to engage with such Promoted Tweets than traditional online ads.



© Kennedy Photography/Alamy

Promoted Trends is the second major Twitter advertising product. “Trends” is a section of the Twitter home page that identifies what people are talking about. A company can place a Promoted Trends banner at the top of the Trends section, and when users click on the banner, they are taken to the follower page for that company or product. A Promoted Trend must be purchased for an entire market for a day (for example, the United States) for a flat fee. In the United States, the fee is now \$200,000, up from \$80,000 when Promoted Trends were first introduced in 2010.

Twitter’s third primary advertising product is Promoted Accounts, which are suggestions to follow various advertiser accounts based on the list of accounts that the user already follows. Like Promoted Tweets, Promoted Accounts can be geo-targeted at both the country level and the local level. Promoted Accounts are priced on a cost-per-follower basis, with advertisers only paying for new followers gained. Prices range from \$.50 to \$2.50. Twitter also offers Enhanced Profile Pages for brands. For a reported \$15,000 to \$25,000, companies get their own banner to display images, and the ability to pin a tweet to the top of the company’s Twitter stream.

In 2013, Twitter began a natural progression into the video ad market. Video clips that include video ads can now be embedded within tweets. Known as the Twitter Amplify program, the program now includes media partners such as CBS, ESPN, Condé Nast, MLB.com, Warner Music, and others. Twitter also launched a television ad targeting product in 2013 that allows marketers to show Promoted Tweets to people who have been tweeting about a television show. In 2014, building on the Amplify program, Twitter announced a beta test of Promoted Video, which allows advertisers to distribute videos on the Twitter platform, and in 2015, it began allowing advertisers to use Promoted Video to link directly to app installations, as well as an ad purchasing feature for videos called “optimized action bidding.” This allows marketers to customize ad purchases to improve their return on investment.

But it is mobile that has proven to be the primary driver of Twitter’s business and the source of most of its revenue. Twitter began testing Promoted Tweets and Promoted Accounts on mobile devices in March 2012, and by June 2012, reported that it was generating the majority of its revenues from ads on mobile devices rather than on its website. Twitter has acquired companies like MoPub and TapCommerce to bolster its mobile capabilities, and in 2015 made its largest acquisition yet, spending \$533 million to acquire digital ad platform TellApart. Twitter hopes that TellApart’s technology will help improve its mobile ad targeting. Currently, Twitter derives over 80% of its advertising revenue from mobile.

Twitter also continues to refine its data mining capability, recognizing that its stockpile of customer sentiment about products, services, and marketing efforts is among its most valuable assets. In 2013, Twitter purchased Big Data startup Lucky Sort and since then has acquired a number of companies such as Topsy Labs and Gnip that will help it improve its ability to provide information about its users’ behavior.

Twitter went public in November 2013 with a valuation of about \$14 billion, raising \$1.8 billion on top of the \$1.2 billion it had previously raised from private investors and venture capital firms. The public offering was viewed as a rousing success, with the stock

SOURCES: “Twitter to Cut Jobs as It Aims For a Turnaround,” by Mike Isaac, *New York Times*, October 27, 2016; “Twitter, Grappling with Anemic Growth, Tries to Bolster Its Advertising Business,” by Mike Isaac, *New York Times*, July 26, 2016; “What Happened to Twitter’s Music Strategy?” by Cherie Hu, *Forbes.com*, May 31, 2016; “Nearly a Year Later, Jack Dorsey’s Twitter Shows Few Signs of a Successful Turnaround,” by Alice Truong, *Quartz.com*, May 30, 2016; “Will The Death of Twitter’s Buy Button Be the End of Social Commerce?” by Natalie Gagliardi, *Zdnet.com*, May 28, 2016; “Report, Twitter Has Stopped Caring About ‘Buy’ Buttons, Just Like the Rest of Us,” by Nate Swanner, *Thenextweb.com*, May 26, 2016; “Twitter Downgraded to Sell: Hope Is Not a Strategy, Research Firm Says,” by Mathew Ingram, *Fortune*, May 24, 2016; “Twitter Narrows Loss, Adds Users, and Misses Revenue Forecast,” by Mike Isaac, *New York Times*, April 26, 2016; “Twitter Gains Rights to Stream Thursday NFL Games,” by Ken Belson and Mike Isaac, *New York Times*, April 5, 2016; “Twitter Will Offer Selected Tweets to Keep Users Coming Back,” by Mike Isaac, *New York Times*, February 10, 2016; “Here’s Another Area Where Twitter Appears to Have Stalled: Tweets Per Day,” by Alexei

price jumping almost 75% on its opening day, despite the fact that at the time, Twitter had not generated a profit. However, its share price has declined significantly from its high of over \$74 in December 2013 down to around \$18 per share as of October 2016, well below its IPO price. Analysts have reiterated serious concerns about Twitter's lack of profitability and anemic growth rate. Only about 20% of U.S. Internet users use Twitter, compared to the over 60% that use Facebook. The vast majority of its users (almost 80%) are located outside the United States, although the United States is the source of over 50% of its ad revenues.

Another issue is user engagement. Research indicates that the vast majority of tweets are generated by a small percentage of users: one study found that the top 15% of users account for 85% of all tweets. This is problematic because Twitter only makes money when a user engages with an ad. User retention is another problem. One study found that Twitter had only a 40% retention rate: 60% of users failed to return the following month. Only about 11% of the accounts created in 2012 are still tweeting. Acknowledging a need for a change in direction, CEO Dick Costolo stepped down in 2015, replaced by co-founder Jack Dorsey.

Twitter recognizes that one of its problems is that it is perceived to be more confusing to use than Facebook. Twitter's first move with Dorsey at the helm was to launch Moments, a feature that packages tweets into thematic groups that are easier to follow. The company also announced upcoming changes to relax the 140-character limit for certain types of content and to provide a curated selection of tweets for users who have been away that might be especially interesting based on their previous activity. Analysts argue that these moves are merely cosmetic.

Dorsey has also vowed to narrow the company's focus on their core service. Twitter is moving away from products and features that don't do enough to enhance the basic user experience. For example, Twitter had hoped that it would become a hub of social e-commerce, and rolled out a Buy Now button in 2014 that allowed users to add products to their Amazon shopping cart. However, in 2016, development on the service has halted due to the users' lukewarm response to the feature. Other services that have failed to take off, such as Twitter's #Music app, have been shelved until further notice. For the time being, Twitter is focusing on improving its video capability, including improving support for its popular Periscope video service. In 2016, Twitter purchased the rights to stream Thursday night NFL games. The ability to stream live events on Twitter is a substantive change in strategy that could help keep users on the site longer.

Despite Dorsey's reshuffling, including restructuring Twitter's board and firing 8% of the workforce, Twitter has yet to reverse its flagging earnings and stagnant growth. In October 2016, Salesforce was rumored to be interested in acquiring Twitter, but decided not to pursue a takeover. Shortly thereafter, Twitter reported yet another loss for the third quarter of the year, and announced that it was cutting an additional 9% of its workforce and shutting down its Vine video app. It is clear Twitter has not yet found a business model that works.

Oreskovic, *Businessinsider.com*, June 15, 2015; "Twitter Is Now Letting Apps Advertise With Video," by Garrett Sloane, *Adweek.com*, July 8, 2015; "Twitter To Pay About \$533 Million For TellApart, Largest Acquisition To Date," by Zach Rodgers, *Adexchanger.com*, April 30, 2015; "Where Did Dick Costolo Go Wrong?" by Erin Griffith, *Fortune*, June 12, 2015; "Twitter's Evolving Plans to Make Money From its Data," by Vindu Goel, *New York Times*, April 11, 2015; "Twitter Launches New Ad Product, Promoted Video, into Beta," by Sarah Perez, *Techcrunch.com*, August 12, 2014; "Twitter Changes Pricing Model for Advertisers," by Mark Bergan, *Adage.com*, August 7, 2014; "Twitter 'Buy Now' Button Appears for First Time," by Kurt Wagner, *Mashable.com*, June 30, 2014; "Twitter Buys TapCommerce, a Mobile Advertising Start-up," by Mike Isaac, *New York Times*, June 30, 2014; "Twitter's Growth Shifts to Developing Countries," by Vindu Goel, *New York Times*, May 27, 2014; "Twitter Pushes Further Into Mobile Ads with MoPub Integration," by Yoree Koh, *Wall Street Journal*, April 17, 2014; "Twitter Acquires Gnip, Bringing a Valuable Data Service In-House," by Ashwin Seshagiri, *New York Times*, April 15, 2014; "Only 11% of New Twitter Users in 2012 Are Still Tweeting," by Yoree Koh, *Wall Street Journal*, March 21, 2014; "Twitter's Big Battle is Indifference," by Yoree Koh, *Wall Street Journal*, February 10, 2014; "A Sneak Peek at Twitter's E-commerce Plans," by Yoree Koh, *Wall Street Journal*, January 31, 2014; "#Wow! Twitter Soars 73% in IPO," by Julianne Pepitone, *Money.cnn.com*, November 7, 2013; "Twitter Amplify Partnerships: Great Content, Great Brands, Great Engagement," by Glenn Brown, *Blog.twitter.com*, May 23, 2013; "Twitter's Latest Buy: Big Data Startup Lucky Sort," by Daniel Terdiman, *News.cnet.com*, May 13, 2013; "Twitter's New Video Plan: Ads, Brought to You by Ads," by Peter Kafka, *Allthingsd.com*, April 16, 2013.

The story of Twitter illustrates the difficulties of turning a good business idea with a huge audience into a successful business model that produces revenues and even profits.

Thousands of firms have discovered that they can spend other people's invested capital much faster than they can get customers to pay for their products or services. In most instances of failure, the business model of the firm is faulty from the beginning. In contrast, successful e-commerce firms have business models that are able to leverage the unique qualities of the Internet, the Web, and the mobile platform, provide customers real value, develop highly effective and efficient operations, avoid legal and social entanglements that can harm the firm, and produce profitable business results. In addition, successful business models must scale. The business must be able to achieve efficiencies as it grows in volume. But what is a business model, and how can you tell if a firm's business model is going to produce a profit?

In this chapter, we focus on business models and basic business concepts that you must be familiar with in order to understand e-commerce.

2.1 E-COMMERCE BUSINESS MODELS

INTRODUCTION

business model

a set of planned activities designed to result in a profit in a marketplace

business plan

a document that describes a firm's business model

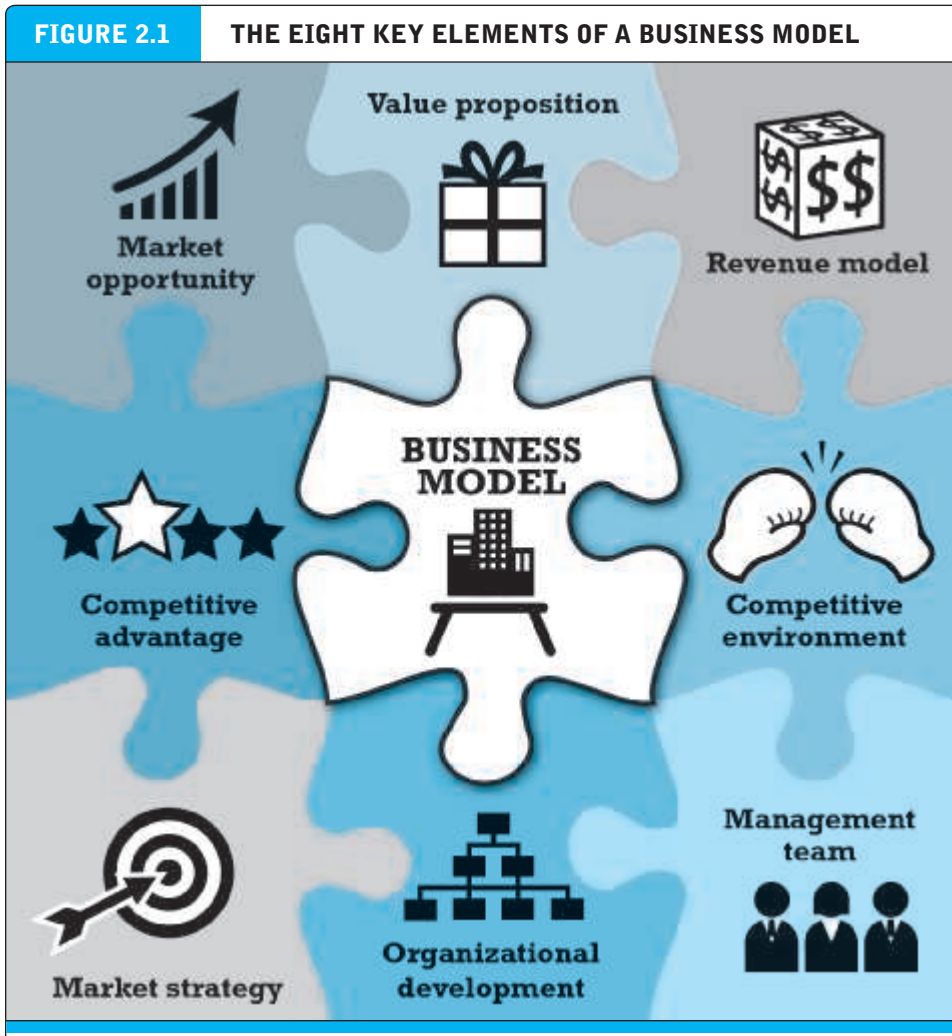
e-commerce business model

a business model that aims to use and leverage the unique qualities of the Internet, the Web, and the mobile platform

A **business model** is a set of planned activities (sometimes referred to as *business processes*) designed to result in a profit in a marketplace. A business model is not always the same as a business strategy, although in some cases they are very close insofar as the business model explicitly takes into account the competitive environment (Magretta, 2002). The business model is at the center of the business plan. A **business plan** is a document that describes a firm's business model. A business plan always takes into account the competitive environment. An **e-commerce business model** aims to use and leverage the unique qualities of the Internet, the Web, and the mobile platform.

EIGHT KEY ELEMENTS OF A BUSINESS MODEL

If you hope to develop a successful business model in any arena, not just e-commerce, you must make sure that the model effectively addresses the eight elements listed in **Figure 2.1**. These elements are **value proposition**, **revenue model**, **market opportunity**, **competitive environment**, **competitive advantage**, **market strategy**, **organizational development**, and **management team**. Many writers focus on a firm's value proposition and revenue model. While these may be the most important and most easily identifiable aspects of a company's business model, the other elements are equally important when evaluating business models and plans, or when attempting to understand why a particular company has succeeded or failed (Kim and Mauborgne, 2000). In the following sections, we describe each of the key business model elements more fully.



A business model has eight key elements. Each element must be addressed if you hope to be successful.

Value Proposition why should the customer buy from you ?

A company's value proposition is at the very heart of its business model. A **value proposition** defines how a company's product or service fulfills the needs of customers (Kambil, Ginsberg, and Bloch, 1998). To develop and/or analyze a firm's value proposition, you need to understand why customers will choose to do business with the firm instead of another company and what the firm provides that other firms do not and cannot. From the consumer point of view, successful e-commerce value propositions include personalization and customization of product offerings, reduction of product search costs, reduction of price discovery costs, and facilitation of transactions by managing product delivery.

value proposition

defines how a company's product or service fulfills the needs of customers

Key Elements of good Value Proposition:-

- Customer
- Problem
- Solution
- Differentiators

For instance, before Amazon existed, most customers personally traveled to book retailers to place an order. In some cases, the desired book might not be available, and the customer would have to wait several days or weeks, and then return to the bookstore to pick it up. Amazon makes it possible for book lovers to shop for virtually any book in print from the comfort of their home or office, 24 hours a day, and to know immediately whether a book is in stock. Amazon's Kindle takes this one step further by making e-books instantly available with no shipping wait. Amazon's primary value propositions are unparalleled selection and convenience.

Revenue Model how will you earn money?

revenue model

describes how the firm will earn revenue, produce profits, and produce a superior return on invested capital

A firm's **revenue model** describes how the firm will earn revenue, generate profits, and produce a superior return on invested capital. We use the terms *revenue model* and *financial model* interchangeably. The function of business organizations is both to generate profits and to produce returns on invested capital that exceed alternative investments. Profits alone are not sufficient to make a company "successful" (Porter, 1985). In order to be considered successful, a firm must produce returns greater than alternative investments. Firms that fail this test go out of existence.

Although there are many different e-commerce revenue models that have been developed, most companies rely on one, or some combination, of the following major revenue models: advertising, subscription, transaction fee, sales, and affiliate.

advertising revenue model

a company provides a forum for advertisements and receives fees from advertisers

In the advertising revenue model, a company that offers content, services, and/or products also provides a forum for advertisements and receives fees from advertisers. Companies that are able to attract the greatest viewership or that have a highly specialized, differentiated viewership and are able to retain user attention ("stickiness") are able to charge higher advertising rates. Yahoo, for instance, derives a significant amount of revenue from display and video advertising.

subscription revenue model

a company offers its users content or services and charges a subscription fee for access to some or all of its offerings

In the subscription revenue model, a company that offers content or services charges a subscription fee for access to some or all of its offerings. For instance, the digital version of *Consumer Reports* provides online and mobile access to premium content, such as detailed ratings, reviews, and recommendations, only to subscribers, who have a choice of paying a \$6.95 monthly subscription fee or a \$30.00 annual fee. Experience with the subscription revenue model indicates that to successfully overcome the disinclination of users to pay for content, the content offered must be perceived as a high-value-added, premium offering that is not readily available elsewhere nor easily replicated. Companies successfully offering content or services online on a subscription basis include eHarmony (dating services), Ancestry (genealogy research), Microsoft's Xbox Live (video games), Pandora, Spotify, and Apple Music (music), Scribd and Amazon's Kindle Unlimited program (e-books), and Netflix and Hulu (television and movies). See **Table 2.1** for examples of various subscription services.

freemium strategy

companies give away a certain level of product or services for free, but then charge a subscription fee for premium levels of the product or service

Recently, a number of companies have been combining a subscription revenue model with a freemium strategy. In a **freemium strategy**, the companies give away a certain level of product or services for free, but then charge a subscription fee for premium levels of the product or service. See the case study, *Freemium Takes Pandora Public*, at the end of the chapter, for a further look at the freemium strategy.

TABLE 2.1 **EXAMPLES OF SUBSCRIPTION SERVICES**

NAME	DESCRIPTION
eHarmony (dating)	<ul style="list-style-type: none"> • Free: Create profile and view profiles of matches • Basic (see photos, send and receive messages): \$180 for 6 months; \$240 for 1 year • Total Connect (Basic plus additional services): \$203 for 6 months; \$287 for 1 year • Premier (Basic/Total Connect plus additional services): \$503/year
Ancestry (genealogical research)	<ul style="list-style-type: none"> • All U.S. records: \$19.99/month or \$99 for 6 months • All U.S. and international records: \$34.99/monthly or \$149 for 6 months
Scribd (e-books)	<ul style="list-style-type: none"> • Unlimited access to “Scribd Select” books and audiobooks, plus 3 books and 1 audiobook of the user’s choice each month for \$8.99/month (over 1 million e-books, audio books, and comic books from which to choose)
Spotify (music)	<ul style="list-style-type: none"> • Many different permutations, depending on device (mobile, tablet, or desktop) and plan chosen (Free, Unlimited, or Premium)

In the **transaction fee revenue model**, a company receives a fee for enabling or executing a transaction. For example, eBay provides an auction marketplace and receives a small transaction fee from a seller if the seller is successful in selling the item. E*Trade, a financial services provider, receives transaction fees each time it executes a stock transaction on behalf of a customer.

In the **sales revenue model**, companies derive revenue by selling goods, content, or services to customers. Companies such as Amazon, L.L.Bean, and Gap all have sales revenue models. A number of companies are also using a **subscription-based sales revenue model**. Birchbox, which offers home delivery of beauty products for a \$10 monthly or \$100 annual subscription price, is one example. Dollar Shave Club, which sells razor blades by subscription and was recently acquired by Unilever for \$1 billion, is another.

In the **affiliate revenue model**, companies that steer business to an “affiliate” receive a referral fee or percentage of the revenue from any resulting sales. For example, MyPoints makes money by connecting companies with potential customers by offering special deals to its members. When they take advantage of an offer and make a purchase, members earn “points” they can redeem for freebies, and MyPoints receives a fee. Community feedback companies typically receive some of their revenue from steering potential customers to websites where they make a purchase.

Table 2.2 summarizes these major revenue models. The *Insight on Society* case, *Foursquare: Check Your Privacy at the Door*, examines some of the issues associated with Foursquare's business and revenue model.

transaction fee revenue model

a company receives a fee for enabling or executing a transaction

sales revenue model

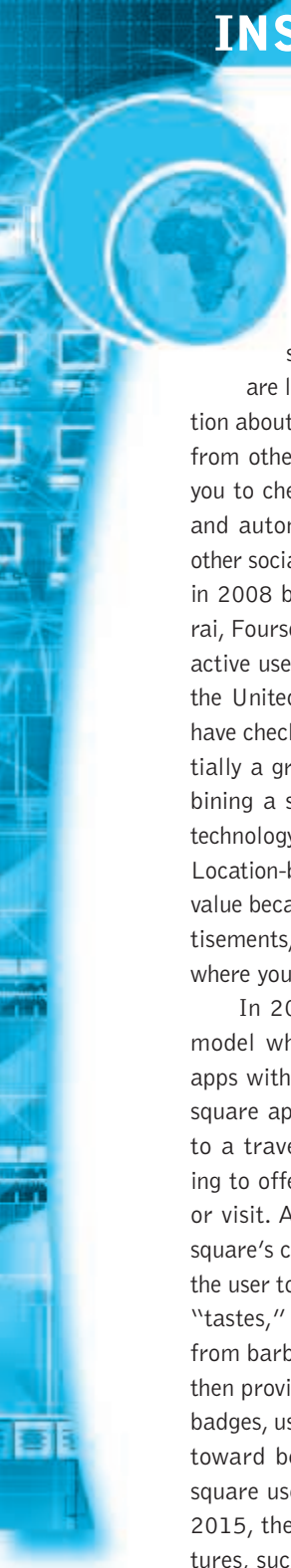
a company derives revenue by selling goods, information, or services

affiliate revenue model

a company steers business to an affiliate and receives a referral fee or percentage of the revenue from any resulting sales

INSIGHT ON SOCIETY

FOURSQUARE: CHECK YOUR PRIVACY AT THE DOOR



Foursquare is one of a host of companies that combine a social network business model with location-based technology. Foursquare offers mobile social applications that know where you are located and can provide you with information about popular spots nearby, as well as reviews from other Foursquare users. Its apps also allow you to check in to a restaurant or other location, and automatically let friends on Facebook and other social networks learn where you are. Founded in 2008 by Dennis Crowley and Naveen Selvadurai, Foursquare has more than 55 million monthly active users worldwide, split fairly evenly between the United States and the rest of the world, who have checked in over 8 billion times. There's potentially a great deal of money to be made by combining a social network with smartphone-based technology that can identify your location precisely. Location-based data has extraordinary commercial value because advertisers can then send you advertisements, coupons, and flash bargains, based on where you are located.

In 2014, Foursquare shook up its business model when it split its app into two separate apps with different focuses. Its redesigned Foursquare app became a recommender system akin to a travel guide, using passive location tracking to offer suggestions to users for where to eat or visit. A separate app, Swarm, absorbed Foursquare's check-in feature. The redesigned app asks the user to identify things he or she likes, known as "tastes," from over 10,000 possibilities (ranging from barbecue to museums to board games), and then provides recommendations. Rather than earn badges, users are encouraged to add tips to work toward becoming an expert. Many loyal Foursquare users were driven away by the change. In 2015, the company added many of the old features, such as status levels, mayorships (awards

offered to users with the most check-ins at a particular location), and leaderboards, back to Swarm. Foursquare's decision was influenced primarily by its continued struggles to find profitability, though it's not for lack of trying. Foursquare has continued to develop in-app advertising products that serve advertising based on users' locations and has formed partnerships with companies like American Express to offer discounts to cardholders after using Foursquare to check-in. Unfortunately for Foursquare, Facebook and seemingly every other social network now offer the ability to check-in and share that information with friends. However, in 2015, Foursquare shifted in a different direction with the launch of its Pinpoint product, an advertising tool that allows marketers unprecedented ability to target users based on its accumulated historical location data and to filter out inaccurate data. Most importantly, Pinpoint can even reach mobile users without the Foursquare app, a major advantage considering the company's relatively low number of in-network users compared to other top social networks.

In 2016, Foursquare is likely to focus more on Pinpoint and other technologies that it can offer other companies than on its flagship check-in app. From 2014 to 2016, Foursquare's revenue doubled on a year-to-year basis, including a 170% increase in its advertising solutions business in 2015. This growth has been driven primarily by data licensing agreements with other tech and social networking giants. For example, in 2014, Foursquare struck just such an agreement with Microsoft, which may use the data to customize Bing on a user-by-user basis with specific search results and advertisements based on their location data. Foursquare has also struck similar deals with Twitter, Google, Yahoo, and Pinterest to provide location-based functions and to share location data, increasing the richness and accuracy of its own data in the process. All of

these partnerships greatly enrich the value of Pinpoint and allow Foursquare to track users that are not even a part of its platform. All of a sudden, Foursquare's "lowly" 55 million users and unimpressive user growth don't matter quite as much. In 2016, Foursquare received \$45 million in new financing, albeit at a much lower valuation than its last round of financing in 2013. Crowley also stepped down as CEO as the company restructured its executive team to focus on continued development of both advertising products as well as techniques to monetize its location data. The company believes that its renewed focus on its advertising products will help it overcome the stigma of its stalled user growth.

As the popularity of location-based services like Foursquare has grown, so too have concerns about privacy. Privacy advocates point out that many apps have no privacy policy, that most of the popular apps transmit location data to their developers, after which the information is not well controlled, and that these services are creating a situation where government, marketers, creditors, and telecommunications firms will end up knowing nearly everything about citizens, including their whereabouts. Many users may not truly understand how much of their location history is available to their friends. A 2016 study indicated that algorithms that analyze Twitter posts in tandem with Foursquare or Instagram posts can identify users' identities with relative ease. One advantage Foursquare does have, though, is that many of its users

are actually interested in having their location tracked and their data collected—users are less likely to revolt when they find that Foursquare is collecting and sharing their data.

The Foursquare app automatically provides Foursquare with the phone's GPS coordinates any time the phone is turned on, even when the app is closed, unless the user specifically opts out of such tracking. In contrast, Facebook's Nearby Friends feature requires users to opt in. Persistent location tracking of this sort further enhances the value of Foursquare's location data. Foursquare claims that the services it provides are a fair trade for the data it collects; privacy experts are concerned that users cannot delete archived location data from Foursquare's servers. Striking a balance between respecting user privacy and continuing to drive profitability will continue to be a challenge for Foursquare moving forward. Signaling a desire to meet its users' demands for privacy, in 2016, Swarm began allowing users to check in without sharing their locations publicly; but at approximately the same time, Foursquare released its Attribution product, which mines daily location information of over 1.3 million Foursquare users who have consented to location tracking in order to determine whether or not the advertising they've seen has actually influenced their purchasing decisions. In July 2016, Foursquare released a digital dashboard for advertising using Attribution that lets marketers drill down into the data even further, with even more detailed audience metrics.

SOURCES: "Foursquare Is Debuting a Dashboard for Its Intriguing Foot Traffic Measurement System," by Christopher Heine, *Adweek.com*, July 25, 2016; "Swarm Now Lets Users Check-In Without Sharing Their Location," by Jordan Crook, *Techcrunch.com*, April 21, 2016; "Location Data From Just Two of Your Apps Is Enough to Reveal Your Identity," by Brian Mastroianni, *Cbsnews.com*, April 14, 2016; "Foursquare 'Attribution' Takes On Nielsen By Selling Foot Traffic From 1.2 Million Daily Mobile Audience," by Kerry Flynn, *Ibetimes.com*, February 22, 2016; "Foursquare's Potentially Game-Changing New Tool Can Measure Foot Traffic Generated by Digital Ads," by Christopher Heine, *Adweek.com*, February 22, 2016; "Inside Foursquare's Plan to Become Profitable," by Andrew Nusca, *Fortune*, January 25, 2016; "Foursquare's Plan to Use Your Data to Make Money—Even If You Aren't a User," by Klint Finley, *Wired.com*, January 19, 2016; "Foursquare Raises \$45 Million, Cutting Its Valuation Nearly in Half," by Mike Isaac, *New York Times*, January 14, 2016; "Swarm Gets Back into the Game with Leaderboards," by Jordan Crook, *Techcrunch.com*, August 20, 2015; "Foursquare by the Numbers: 60M Registered Users, 50M MAUs, and 75M Tips to Date," by Harrison Weber and Jordan Novet, *Venturebeat.com*, August 18, 2015; "Foursquare Returns to Its Roots in Bid to Win Back Users," by Jason Cipriani, *Fortune*, May 13, 2015; "Foursquare Unveils Pinpoint for Location-Based Ad Targeting," by Melanie White, *Clickz.com*, April 14, 2015; "Foursquare Unveils Pinpoint to Show You Ads Based on Where You've Been," by Harrison Weber, *Venturebeat.com*, April 14, 2015; "Why Twitter and Foursquare Just Struck a Deal," by Erin Griffith, *Fortune*, March 23, 2015; "Radical New Foursquare App Thinks You Want Even Less Privacy," by Jason Cipriani, *Wired.com*, August 6, 2014; "Foursquare Now Tracks Users Even When the App is Closed," by Douglas Macmillan, *Wall Street Journal*, August 6, 2014; "Foursquare Updates Swarm to Soothe the Check-in Blues," by Caitlin McGarry, *Techhive.com*, July 8, 2014; "How Foursquare Uses Location Data to Target Ads on PCs, Phones," by Cotton Delo, *Adage.com*, February 27, 2014; "With Foursquare Deal, Microsoft Aims for Supremacy in Hyper-Local Search," by Ryan Tate, *Wired.com*, February 5, 2014.

TABLE 2.2 FIVE PRIMARY REVENUE MODELS		
REVENUE MODEL	EXAMPLES	REVENUE SOURCE
Advertising	Yahoo	Fees from advertisers in exchange for advertisements
Subscription	eHarmony Consumer Reports Online Netflix	Fees from subscribers in exchange for access to content or services
Transaction Fee	eBay E*Trade	Fees (commissions) for enabling or executing a transaction
Sales	Amazon L.L.Bean Birchbox iTunes	Sales of goods, information, or services
Affiliate	MyPoints	Fees for business referrals

market opportunity
refers to the company's intended marketplace and the overall potential financial opportunities available to the firm in that marketplace

marketplace
the area of actual or potential commercial value in which a company intends to operate

Niche & Mass Market
Niche Market is a smaller segment of a larger market where customers have more specific needs and wants.

competitive environment
refers to the other companies operating in the same marketplace selling similar products

what marketplace do you intend to serve and what is its size?

Market Opportunity

The term **market opportunity** refers to the company's intended **marketplace** (i.e., an area of actual or potential commercial value) and the overall potential financial opportunities available to the firm in that marketplace. The market opportunity is usually divided into smaller **market niches**. The realistic market opportunity is defined by the revenue potential in each of the market niches where you hope to compete.

For instance, let's assume you are analyzing a **software training company** that creates online software-learning systems for sale to businesses. The overall size of the software training market for all market segments is approximately \$70 billion. The overall market can be broken down, however, into two major market segments: **instructor-led training products**, which comprise about 70% of the market (\$49 billion in revenue), and **computer-based training**, which accounts for 30% (\$21 billion). There are further market niches within each of those major market segments, such as the **Fortune 500 computer-based training market** and the **small business computer-based training market**. Because the firm is a start-up firm, it cannot compete effectively in the large business, **computer-based training market** (about \$15 billion). Large brand-name training firms dominate this niche. The start-up firm's real market opportunity is to sell to the thousands of **small business firms** that spend about \$6 billion on computer-based software training. This is the size of the firm's realistic market opportunity (see **Figure 2.2**).

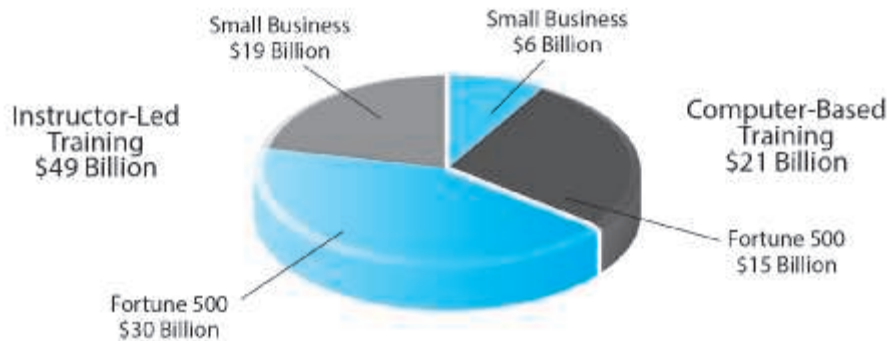
Competitive Environment

who else occupies your intended marketplace?

A firm's **competitive environment** refers to the other companies selling similar products and operating in the same marketplace. It also refers to the presence of substitute products and potential new entrants to the market, as well as the power of customers and suppliers over your business. We discuss the firm's environment

FIGURE 2.2

MARKETSPACE AND MARKET OPPORTUNITY IN THE SOFTWARE TRAINING MARKET



Marketspaces are composed of many market segments. Your realistic market opportunity will typically focus on one or a few market segments.

later in the chapter. The competitive environment for a company is influenced by several factors: how many competitors are active, how large their operations are, what the market share of each competitor is, how profitable these firms are, and how they price their products.

Firms typically have both direct and indirect competitors. Direct competitors are companies that sell very similar products and services into the same market segment. For example, Priceline and Travelocity, both of whom sell discount airline tickets online, are direct competitors because both companies sell identical products—cheap tickets. Indirect competitors are companies that may be in different industries but still compete indirectly because their products can substitute for one another. For instance, automobile manufacturers and airline companies operate in different industries, but they still compete indirectly because they offer consumers alternative means of transportation. CNN, a news outlet, is an indirect competitor of ESPN, not because they sell identical products, but because they both compete for consumers' time online.

The existence of a large number of competitors in any one segment may be a sign that the market is saturated and that it may be difficult to become profitable. On the other hand, a lack of competitors could signal either an untapped market niche ripe for the picking, or a market that has already been tried without success because there is no money to be made. Analysis of the competitive environment can help you decide which it is.

Competitive Advantage

what special advantages does your firm bring to the marketplace?

Firms achieve a **competitive advantage** when they can produce a superior product and/or bring the product to market at a lower price than most, or all, of their

competitive advantage

achieved by a firm when it can produce a superior product and/or bring the product to market at a lower price than most, or all, of its competitors

competitors (Porter, 1985). Firms also compete on scope. Some firms can develop global markets, while other firms can develop only a national or regional market. Firms that can provide superior products at the lowest cost on a global basis are truly advantaged. **what are some of the specific ways that a company can obtain a competitive advantages**

1 Firms achieve competitive advantages because they have somehow been able to obtain differential access to the factors of production that are denied to their competitors—at least in the short term (Barney, 1991). Perhaps the firm has been able to obtain very favorable terms from suppliers, shippers, or sources of labor. Or perhaps the firm has more experienced, knowledgeable, and loyal employees than any competitors. Maybe the firm has a patent on a product that others cannot imitate, or access to investment capital through a network of former business colleagues or a brand name and popular image that other firms cannot duplicate. An asymmetry exists whenever one participant in a market has more resources—financial backing, knowledge, information, and/or power—than other participants. Asymmetries lead to some firms having an edge over others, permitting them to come to market with better products, faster than competitors, and sometimes at lower cost. **lack of equality or equivalence**

For instance, when Apple announced iTunes, a service offering legal, downloadable individual song tracks for 99 cents a track that would be playable on any digital device with iTunes software, the company had better-than-average odds of success simply because of Apple's prior success with innovative hardware designs, and the large stable of music firms that Apple had meticulously lined up to support its online music catalog. Few competitors could match the combination of cheap, legal songs and powerful hardware to play them on.

2 One rather unique competitive advantage derives from being a first mover. A first-mover advantage is a competitive market advantage for a firm that results from being the first into a marketplace with a serviceable product or service. If first movers develop a loyal following or a unique interface that is difficult to imitate, they can sustain their first-mover advantage for long periods (Arthur, 1996). Amazon provides a good example. However, in the history of technology-driven business innovation, most first movers often lack the complementary resources needed to sustain their advantages, and often follower firms reap the largest rewards (Rigdon, 2000; Teece, 1986). Indeed, many of the success stories we discuss in this book are those of companies that were slow followers—businesses that gained knowledge from the failure of pioneering firms and entered into the market late.

3 Some competitive advantages are called “unfair.” An unfair competitive advantage occurs when one firm develops an advantage based on a factor that other firms cannot purchase (Barney, 1991). For instance, a brand name cannot be purchased and is in that sense an “unfair” advantage. Brands are built upon loyalty, trust, reliability, and quality. Once obtained, they are difficult to copy or imitate, and they permit firms to charge premium prices for their products.

In perfect markets, there are no competitive advantages or asymmetries because all firms have access to all the factors of production (including information and knowledge) equally. However, real markets are imperfect, and asymmetries leading to competitive advantages do exist, at least in the short term. Most competitive

Examples

asymmetry

exists whenever one participant in a market has more resources than other participants

first-mover advantage

a competitive market advantage for a firm that results from being the first into a marketplace with a serviceable product or service

complementary resources

resources and assets not directly involved in the production of the product but required for success, such as marketing, management, financial assets, and reputation

unfair competitive advantage

occurs when one firm develops an advantage based on a factor that other firms cannot purchase

perfect market

a market in which there are no competitive advantages or asymmetries because all firms have equal access to all the factors of production

advantages are short term, although some can be sustained for very long periods. But not forever. In fact, many respected brands fail every year.

Companies are said to **leverage** their competitive assets when they use their competitive advantages to achieve more advantage in surrounding markets. For instance, Amazon's move into the online grocery business leverages the company's huge customer database and years of e-commerce experience.

Market Strategy

how do you plan to promote your products or services to attract your target audience?

No matter how tremendous a firm's qualities, its marketing strategy and execution are often just as important. The best business concept, or idea, will fail if it is not properly marketed to potential customers.

Everything you do to promote your company's products and services to potential customers is known as marketing. **Market strategy** is the plan you put together that details exactly how you intend to enter a new market and attract new customers.

For instance, Twitter, YouTube, and Pinterest have a social network marketing strategy that encourages users to post their content for free, build personal profile pages, contact their friends, and build a community. In these cases, the customer becomes part of the marketing staff!

Organizational Development

What types of organizational structures within the firm are necessary to carry out the business plan?

Although many entrepreneurial ventures are started by one visionary individual, it is rare that one person alone can grow an idea into a multi-million dollar company. In most cases, fast-growth companies—especially e-commerce businesses—need employees and a set of business procedures. In short, all firms—new ones in particular—need an organization to efficiently implement their business plans and strategies. Many e-commerce firms and many traditional firms that attempt an e-commerce strategy have failed because they lacked the organizational structures and supportive cultural values required to support new forms of commerce (Kanter, 2001).

Companies that hope to grow and thrive need to have a plan for **organizational development** that describes how the company will organize the work that needs to be accomplished. Typically, work is divided into functional departments, such as production, shipping, marketing, customer support, and finance. Jobs within these functional areas are defined, and then recruitment begins for specific job titles and responsibilities. Typically, in the beginning, generalists who can perform multiple tasks are hired. As the company grows, recruiting becomes more specialized. For instance, at the outset, a business may have one marketing manager. But after two or three years of steady growth, that one marketing position may be broken down into seven separate jobs done by seven individuals.

For instance, eBay founder Pierre Omidyar started an online auction site, according to some sources, to help his girlfriend trade Pez dispensers with other collectors, but within a few months the volume of business had far exceeded what he alone could handle. So he began hiring people with more business experience to help out. Soon the company had many employees, departments, and managers who were responsible for overseeing the various aspects of the organization.

leverage

when a company uses its competitive advantages to achieve more advantage in surrounding markets

market strategy

the plan you put together that details exactly how you intend to enter a new market and attract new customers

organizational development

plan that describes how the company will organize the work that needs to be accomplished

management team

employees of the company responsible for making the business model work

Management Team

what kind of backgrounds and experiences should the company's leaders have?

Arguably, the single most important element of a business model is the **management team** responsible for making the model work. A strong management team gives a model instant credibility to outside investors, immediate market-specific knowledge, and experience in implementing business plans. A strong management team may not be able to salvage a weak business model, but the team should be able to change the model and redefine the business as it becomes necessary.

Eventually, most companies get to the point of having several senior executives or managers. How skilled managers are, however, can be a source of competitive advantage or disadvantage. The challenge is to find people who have both the experience and the ability to apply that experience to new situations.

To be able to identify good managers for a business start-up, first consider the kinds of experiences that would be helpful to a manager joining your company. What kind of technical background is desirable? What kind of supervisory experience is necessary? How many years in a particular function should be required? What job functions should be fulfilled first: marketing, production, finance, or operations? Especially in situations where financing will be needed to get a company off the ground, do prospective senior managers have experience and contacts for raising financing from outside investors?

Table 2.3 summarizes the eight key elements of a business model and the key questions that must be answered in order to successfully develop each element.

RAISING CAPITAL

Raising capital is one of the most important functions for a founder of a start-up business and its management team. Not having enough capital to operate effectively is a primary reason why so many start-up businesses fail. Many entrepreneurs initially "bootstrap" to get a business off the ground, using personal funds derived from savings,

TABLE 2.3 KEY ELEMENTS OF A BUSINESS MODEL	
COMPONENTS	KEY QUESTIONS
Value proposition	Why should the customer buy from you?
Revenue model	How will you earn money?
Market opportunity	What marketplace do you intend to serve, and what is its size?
Competitive environment	Who else occupies your intended marketplace?
Competitive advantage	What special advantages does your firm bring to the marketplace?
Market strategy	How do you plan to promote your products or services to attract your target audience?
Organizational development	What types of organizational structures within the firm are necessary to carry out the business plan?
Management team	What kinds of experiences and background are important for the company's leaders to have?

TABLE 2.4

KEY ELEMENTS OF AN ELEVATOR PITCH

ELEMENT	DESCRIPTION
Introduction	Your name and position; your company's name, and a tagline in which you compare what your company does to a well-known company. Example: "My name is X, I am the founder of Y, and we are the Uber/Amazon of Z."
Background	The origin of your idea and the problem you are trying to solve.
Industry size/market opportunity	Brief facts about the (hopefully very large) size of the market.
Revenue model/numbers/growth metrics	Insight into your company's revenue model and results thus far, how fast it is growing, and early adopters, if there are any.
Funding	The amount of funds you are seeking and what it will help you achieve.
Exit strategy	How your investors will achieve a return on their investment.

credit card advances, home equity loans, or from family and friends. Funds of this type are often referred to as **seed capital**. Once such funds are exhausted, if the company is not generating enough revenue to cover operating costs, additional capital will be needed. **Traditional sources of capital** include **incubators**, **commercial banks**, **angel investors**, **venture capital firms**, and **strategic partners**. One of the most important aspects of raising capital is the ability **to boil down the elements of the company's business plan into an elevator pitch**, a short two-to-three minute (about the length of an elevator ride, giving rise to its name) presentation aimed at **convincing investors to invest**. **Table 2.4** lists the key elements of an elevator pitch.

Incubators (sometimes also referred to as accelerators) such as Y Combinator (profiled in Chapter 1's *Insight on Business* case) typically provide a small amount of funding, but more importantly, also provide an array of services to start-up companies that they select to participate in their programs, such as business, technical, and marketing assistance, as well as introductions to other sources of capital. Well-known incubator programs include **TechStars**, **DreamIt**, and **Capital Factory**.

Obtaining a loan from a commercial bank is often difficult for a start-up company without much revenue, but it may be worthwhile to investigate programs offered by the U.S. Small Business Administration, and its state or local equivalents. The advantage of obtaining capital in the form of a loan (debt) is that, although it must be repaid, it does not require an entrepreneur to give up any ownership of the company.

Angel investors are typically wealthy individuals (or a group of individuals) who invest their own money in an exchange for an equity share in the stock in the business. In general, angel investors make smaller investments (typically \$1 million or less) than venture capital firms, are interested in helping a company grow and succeed, and invest on relatively favorable terms compared to later stage investors. **The first round of external investment in a company is sometimes referred to as Series A financing.**

seed capital

typically, an entrepreneur's personal funds derived from savings, credit card advances, home equity loans, or from family and friends

elevator pitch

short two-to-three minute presentation aimed at convincing investors to invest

incubators

typically provide a small amount of funding and also an array of services to start-up companies

angel investors

typically wealthy individuals or a group of individuals who invest their own money in exchange for an equity share in the stock of a business; often are the first outside investors in a start-up

venture capital investors

typically invest funds they manage for other investors; usually later-stage investors

crowdfunding

involves using the Internet to enable individuals to collectively contribute money to support a project

Venture capital investors typically become more interested in a start-up company once it has begun attracting a large audience and generating some revenue, even if it is not profitable. **Venture capital investors** invest funds they manage for other investors such as investment banks, pension funds, insurance companies, or other businesses, and usually want to obtain a larger stake in the business and exercise more control over the operation of the business. Venture capital investors also typically want a well-defined “exit strategy,” such as a plan for an initial public offering or acquisition of the company by a more established business within a relatively short period of time (typically 3 to 7 years), that will enable them to obtain an adequate return on their investment. Venture capital investment often ultimately means that the founder(s) and initial investors will no longer control the company at some point in the future.

Crowdfunding involves using the Internet to enable individuals to collectively contribute money to support a project. The concepts behind crowdfunding have been popularized by Kickstarter and Indiegogo, but they were not able to be used for equity investments in for-profit companies in the United States due to securities regulations. However, the passage of the Jumpstart Our Business Startups (JOBS) Act in 2012 and issuance of regulations by the Securities and Exchange Commission in July 2013 has enabled companies to use the Internet to solicit wealthy (“accredited”) investors to invest in small and early-stage start-ups in exchange for stock. Regulation A+, which enables equity crowdfunding investments by non-accredited investors (people with a net worth of less than \$1 million and who earned less than \$200,000 a year in the previous two years), took effect in June 2015. Regulations implementing even broader-based equity crowdfunding authorized by the JOBS Act, which allow investments by people with annual income or net worth of less than \$100,000, also recently took effect, in May 2016. See the *Insight on Business* case, *Crowdfunding Takes Off*, for a further look at the issues surrounding crowdfunding.

CATEGORIZING E-COMMERCE BUSINESS MODELS: SOME DIFFICULTIES

There are many e-commerce business models, and more are being invented every day. The number of such models is limited only by the human imagination, and our list of different business models is certainly not exhaustive. However, despite the abundance of potential models, it is possible to identify the major generic types (and subtle variations) of business models that have been developed for the e-commerce arena and describe their key features. It is important to realize, however, that there is no one correct way to categorize these business models.

Our approach is to categorize business models according to the different major e-commerce sectors—B2C and B2B—in which they are utilized. You will note, however, that fundamentally similar business models may appear in more than one sector. For example, the business models of online retailers (often called e-tailers) and e-distributors are quite similar. However, they are distinguished by the market focus of the sector in which they are used. In the case of e-tailers in the B2C sector, the business model focuses on sales to the individual consumer, while in the case of the e-distributor, the business model focuses on sales to another business. Many companies use a variety of

INSIGHT ON BUSINESS

CROWDFUNDING TAKES OFF



Think you have the next big idea but lack the resources to make it happen? Crowdfunding sites might be your best shot. Sites such as Kickstarter, Indiegogo, RocketHub, and Tilt have led the growth of crowdfunding from \$530 million in 2009 to over \$34 billion in 2015. A World Bank study predicts that capital raised via crowdfunding will exceed \$93 billion by 2025. The Internet is the ideal medium for crowdfunding because it allows individuals and organizations in need of funds and potential backers to find one another around the globe.

How do sites like Kickstarter and Indiegogo work? The idea is simple—an inventor, artist, or activist looking to raise money for a project uses the site to create a page for that project. People can pledge to support the project, but at Kickstarter, money actually only changes hands once the project fully reaches its funding goal (other sites, such as Indiegogo and RocketHub, allow project creators to keep the money they raise even if they do not achieve their goal). The sites take a small commission, usually about 5%, on completed projects. Backers often receive some type of reward, often corresponding to the size of their contribution to the project.

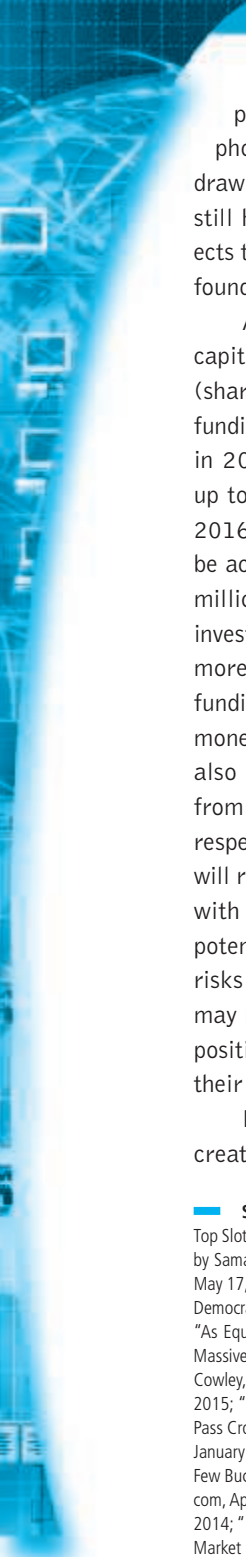
Crowdfunding is quickly becoming a mainstay in the development of movies, video games, art installations, and other types of projects. For instance, among the most funded Kickstarter projects to date are Pebble, a customizable e-paper watch that connects to a smartphone (over \$33 million raised across several campaigns) and Coolest Cooler, a cooler with a waterproof Bluetooth speaker, USB charger and other high tech features (\$13.3 million). Several of the biggest

Kickstarter projects have been movie projects that struggled to gain traction at Hollywood studios, like the *Veronica Mars* movie project (\$5.7 million) and a project to reboot the popular educational TV show *Reading Rainbow*, which garnered over \$5 million in financing in 2015. In 2014, a man from Ohio solicited \$10 in donations to make a batch of potato salad as a joke, but after his campaign went viral, he raised over \$55,000, much of which he used to support local charities. The applications for crowdfunding are limited only by the imagination.

Successful crowdfunding projects typically share some common elements. One of the most important is a clear and concise presentation of the idea, especially through the use of video. The crowdfunding campaign is in many ways similar to presenting a business plan, and should touch on the same eight elements of a business model, such as the project's value proposition, its target market, and so on. A whole ecosystem of video producers, editors, and other services has sprung up to support crowdfunding projects.

Not every crowdfunding project gets off the ground—Kickstarter reports that only about 35% of its approximately 308,000 projects thus far have reached their funding goals. Sometimes projects that do get off the ground simply flame out, disappointing their backers. For instance, the Coolest Cooler has been marred by price increases, delays in production, and failure to deliver the product to its original backers, despite shipping it to those who pay full retail price on Amazon. Another high profile Kickstarter, fledgling drone manufacturer Zano, went bankrupt before ever completing its product, despite raising \$3.4 million. Kickstarter now requires fundraisers to

(continued)



disclose the risks associated with their project, and for inventions, now requires photos of prototype products instead of simply drawings, simulations, or renderings. But backers still have no real recourse with respect to projects that never get off the ground or unresponsive founders.

A new use of crowdfunding is to provide seed capital for startup companies in return for equity (shares) in the company, known as equity crowdfunding. Under the JOBS Act passed by Congress in 2012, a company will be able to crowdfund up to \$1 million over a 12-month period, and in 2016, the rules requiring potential investors to be accredited (having a net worth of at least \$1 million dollars) were relaxed to allow smaller investors to purchase equity stakes of \$2,000 or more. Twenty-five states have their own crowdfunding rules that allow local businesses to raise money in this way, and the 2016 regulations will also fix a loophole preventing these businesses from advertising to investors from outside their respective states. However, equity crowdfunding will require extensive compliance from businesses, with steep penalties for any irregularities, and potential investors will be subject to all the same risks that professional investors experience, but may put themselves in more precarious financial positions as a result. They'll also be forced to hold their investments for at least one year.

Kickstarter currently has no plans to allow creators to offer equity in Kickstarter projects,

believing that equity crowdfunding is fundamentally different from the projects on its site, which focus less on profits and more on ideas and social issues. In the meantime, many companies, such as Indiegogo, Crowdfunder, AngelList, and StartEngine are laying the groundwork for an expected explosion of activity. Indiegogo in particular has been open about its support for the JOBS act and is currently working on implementing it as an option on its site in the near future. When it does, it's likely to immediately become the dominant player in the industry thanks to its 15 million monthly visitors. Niche companies are also springing up, with varying degrees of success. For instance, SeedInvest is a company that caters to investors who may have concerns about crowdfunding privacy by offering better privacy controls. CircleUp is focused on consumer products. As crowdfunding becomes more widely recognized by the general public, more specialty sites such as these are likely to spring up. However, studies from MIT and the College of William and Mary suggest that equity crowdfunding isn't as likely to lead to positive outcomes for smaller investors. Many of the highest quality startups won't need to use equity crowdfunding and will instead pursue more traditional venture capitalists, and smaller investors may be more likely to fall prey to misleading claims from businesses seeking funding. It's likely that more regulations will need to be developed to protect smaller equity crowdfunding investors in coming months and years.

SOURCES: "Indiegogo Could Soon Dominate Equity Crowdfunding," by Jeremy Quittner, *Fortune*, July 5, 2016; "Latest Pebble Campaign Snags the Top Slot on Kickstarter," by Haje Jan Kamps, *Techcrunch.com*, June 30, 2016; "New Crowdfunding Rules Could Do More Harm Than Good for Some Startups," by Samantha Drake, *Forbes*, June 27, 2016; "Equity Crowdfunding is Here—And It Could Be Terrible for Indie Filmmakers," by Chris O'Falt, *Indiewire.com*, May 17, 2016; "New Crowdfunding Rules Let the Small Fry Swim with Sharks," by Stacy Cowley, *New York Times*, May 14, 2016; "Can Equity Crowdfunding Democratize Access to Capital and Investment Opportunities?," by Christian Catalini, Catherine Fazio, and Fiona Murray, MIT Innovation Initiative, May 2016; "As Equity Crowdfunding Debuts in U.S., Will More Regulations Follow?," by Jeff Engel, *Xconomy.com*, March 25, 2016; "Trouble on Kickstarter as Two Massive Projects Hit the Rocks," by Alex Hern, *The Guardian*, November 19, 2015; "S.E.C. Gives Small Investors Access to Equity Crowdfunding," by Stacy Cowley, *New York Times*, October 30, 2015; "Equity Crowdfunding: A Market for Lemons?," by Darian M. Ibrahim, College of William & Mary Law School, 2015; "Indiegogo Is Getting Ready for Equity Crowdfunding," by Harry McCracken, *Fast Company*, October 2015; "Tired of Waiting for U.S. to Act, States Pass Crowdfunding Laws and Rules," by Stacy Cowley, *New York Times*, June 3, 2015; "Keeping Up With Kickstarter," by Stephen Heyman, *New York Times*, January 15, 2015; "Why Investors Are Pouring Millions into Crowdfunding," by Katherine Noyes, *Fortune*, April 17, 2014; "Invest in Next Facebook... For a Few Bucks," by Patrick M. Sheridan, *CNNMoney.com*, April 14, 2014; "How You'll Fund—And Wildly Profit From—The Next Oculus Rift," by Ryan Tate, *Wired.com*, April 4, 2014; "If You Back a Kickstarter Project That Sells for \$2 Billion, Do You Deserve to Get Rich?," by Adrienne Jeffries, *Theverge.com*, March 28, 2014; "Crowdfunding Tips for Turning Inspiration into Reality," by Kate Murphy, *New York Times*, January 22, 2014; "World Bank: Crowdfunding Investment Market to Hit \$93 Billion by 2025," by Richard Swart, *PBS.org*, December 10, 2013; "SEC Finally Moves on Equity Crowdfunding, Phase 1," by Chance Barnett, *Forbes.com*, July 19, 2013.

different business models as they attempt to extend into as many areas of e-commerce as possible. We look at B2C business models in Section 2.2 and B2B business models in Section 2.3.

A business's technology platform is sometimes confused with its business model. For instance, "mobile e-commerce" refers to the use of mobile devices and cellular and wide area networks to support a variety of business models. Commentators sometimes confuse matters by referring to mobile e-commerce as a distinct business model, which it is not. All of the basic business models we discuss below can be implemented on both the traditional Internet/Web and mobile platforms. Likewise, although they are sometimes referred to as such, social e-commerce and local e-commerce are not business models in and of themselves, but rather subsectors of B2C and B2B e-commerce in which different business models can operate.

You will also note that some companies use multiple business models. For instance, Amazon has multiple business models: it is an e-retailer, content provider, market creator, e-commerce infrastructure provider, and more. eBay is a market creator in the B2C and C2C e-commerce sectors, using both the traditional Internet/Web and mobile platforms, as well as an e-commerce infrastructure provider. Firms often seek out multiple business models as a way to leverage their brands, infrastructure investments, and assets developed with one business model into new business models.

Finally, no discussion of e-commerce business models would be complete without mention of a group of companies whose business model is focused on providing the infrastructure necessary for e-commerce companies to exist, grow, and prosper. These are the e-commerce enablers. They provide the hardware, operating system software, networks and communications technology, applications software, web design, consulting services, and other tools required for e-commerce (see **Table 2.5** on page 72). While these firms may not be conducting e-commerce per se (although in many instances, e-commerce in its traditional sense is in fact one of their sales channels), as a group they have perhaps profited the most from the development of e-commerce. We discuss many of these players in the following chapters.

2.2 MAJOR BUSINESS-TO-CONSUMER (B2C) BUSINESS MODELS

Business-to-consumer (B2C) e-commerce, in which online businesses seek to reach individual consumers, is the most well-known and familiar type of e-commerce. **Table 2.6** illustrates the major business models utilized in the B2C arena.

1 E-TAILER Online version of traditional retailer

Online retail stores, often called **e-tailers**, come in all sizes, from giant Amazon to tiny local stores. E-tailers are similar to the typical bricks-and-mortar storefront, except that customers only have to connect to the Internet or use their smartphone to place an order. Some e-tailers, which are referred to as "bricks-and-clicks," are subsidiaries or

e-tailer
online retail store

TABLE 2.5 E-COMMERCE ENABLERS

INFRASTRUCTURE	PLAYERS
Hardware: Web Servers	HP • Dell • Lenovo
Software: Web Server Software	Microsoft • IBM • Red Hat Linux (Apache) • Oracle
Cloud Providers	Amazon Web Services • Google • IBM • Rackspace
Hosting Services	Rackspace • WebIntellects • 1&1 • HostGator • Hostway
Domain Name Registration	GoDaddy • Network Solutions • Dotster
Content Delivery Networks	Akamai • Limelight
Site Design	Weebly • Wix • Squarespace
E-commerce Platform Providers	Magento • IBM • Oracle • Salesforce
Mobile Commerce Hardware Platform	Apple • Samsung • LG
Mobile Commerce Software Platform	Apple • Google • Adobe • Usablenet • Unbound Commerce
Streaming, Rich Media, Online Video	Adobe • Apple • Webcollage
Security and Encryption	VeriSign • Check Point • GeoTrust • Entrust • Thawte • Intel Security
Payment Systems	PayPal • Authorize.net • Chase Paymentech • Cybersource
Web Performance Management	Compuware • SmartBear • Keynote
Comparison Engine Feeds/Marketplace Management	ChannelAdvisor • CommerceHub • CPC Strategy
Customer Relationship Management	Oracle • SAP • Salesforce • Microsoft Dynamics
Order Management	JDA Software • Jagged Peak • Monsoon Commerce
Fulfillment	JDA Software • Jagged Peak • CommerceHub
Social Marketing	Buffer • HootSuite • SocialFlow
Search Engine Marketing	iProspect • ChannelAdvisor • Merkle
E-mail Marketing	Constant Contact • Experian CheetahMail • Bronto Software • MailChimp
Affiliate Marketing	CJ Affiliate • Rakuten LinkShare
Customer Reviews and Forums	Bazaarvoice • PowerReviews • BizRate
Live Chat/Click-to-Call	LivePerson • BoldChat • Oracle
Web Analytics	Google Analytics • Adobe Analytics • IBM Digital Analytics • Webtrends

E- Retailer Variations:
 1- Bricks and Click - Mixed
 2- Virtual Merchant
 3- Manufacture- direct
 4- Cataloges Merchant

divisions of existing physical stores and carry the same products. REI, JCPenney, Barnes & Noble, Walmart, and Staples are examples of companies with complementary online stores. Others, however, operate only in the virtual world, without any ties to physical locations. Amazon, Blue Nile, and Bluefly are examples of this type of e-tailer. Several other variations of e-tailers—such as online versions of direct mail catalogs, online malls, and manufacturer-direct online sales—also exist.

Given that the overall retail market in the United States in 2016 is estimated to be around \$4.8 trillion, the market opportunity for e-tailers is very large. Every Internet and smartphone user is a potential customer. Customers who feel time-starved are even better prospects, because they want shopping solutions that will eliminate the

TABLE 2.6 B2C BUSINESS MODELS

BUSINESS MODEL	VARIATIONS	EXAMPLES	DESCRIPTION	REVENUE MODELS
E-tailer	Virtual Merchant	Amazon Blue Nile Bluefly	Online version of retail store, where customers can shop at any hour of the day or night without leaving their home or office	Sales of goods
	Bricks-and-Clicks	Walmart Sears	Online distribution channel for a company that also has physical stores	Sales of goods
	Catalog Merchant	L.L.Bean LillianVernon	Online version of direct mail catalog	Sales of goods
	Manufacturer-Direct	Dell Mattel	Manufacturer uses online channel to sell direct to customer	Sales of goods
Community Provider		Facebook LinkedIn Twitter Pinterest	Sites where individuals with particular interests, hobbies, common experiences, or social networks can come together and "meet" online	Advertising, subscription, affiliate referral fees
Content Provider		Wall Street Journal CNN ESPN Netflix Apple Music	Offers customers newspapers, magazines, books, film, television, music, games, and other forms of online content	Advertising, subscription fees, sales of digital goods
Portal	Horizontal/General	Yahoo AOL MSN Facebook	Offers an integrated package of content, search, and social network services: news, e-mail, chat, music downloads, video streaming, calendars, etc. Seeks to be a user's home base	Advertising, subscription fees, transaction fees
	Vertical/Specialized (Vortal)	Sailnet	Offers services and products to specialized marketplace	Advertising, subscription fees, transaction fees
	Search	Google Bing Ask	Focuses primarily on offering search services	Advertising, affiliate referral
Transaction Broker		E*Trade Expedia Monster Travelocity Orbitz	Processors of online sales transactions, such as stockbrokers and travel agents, that increase customers' productivity by helping them get things done faster and more cheaply	Transaction fees
Market Creator		eBay Etsy Amazon Priceline	Businesses that use Internet technology to create markets that bring buyers and sellers together	Transaction fees
Service Provider		VisaNow Wave RocketLawyer	Companies that make money by selling users a service, rather than a product	Sales of services

barriers to entry

the total cost of entering a new marketplace

need to drive to the mall or store (Bellman, Lohse, and Johnson, 1999). The e-tail revenue model is product-based, with customers paying for the purchase of a particular item.

This sector, however, is extremely competitive. Because **barriers to entry** (the total cost of entering a new marketplace) into the e-tail market are low, tens of thousands of small e-tail shops have sprung up. Becoming profitable and surviving is very difficult, however, for e-tailers with no prior brand name or experience. The e-tailer's challenge is differentiating its business from existing competitors.

Companies that try to reach every online consumer are likely to deplete their resources quickly. Those that develop a niche strategy, clearly identifying their target market and its needs, are best prepared to make a profit. Keeping expenses low, selection broad, and inventory controlled is key to success in e-tailing, with inventory being the most difficult to gauge. Online retail is covered in more depth in Chapter 9.

2

COMMUNITY PROVIDER**community provider**

creates an online environment where people with similar interests can transact (buy and sell goods); share interests, photos, and videos; communicate with like-minded people; and receive interest-related information

Although community providers are not a new phenomenon, the Internet has made such sites for like-minded individuals to meet and converse much easier, without the limitations of geography and time to hinder participation. **Community providers** create an online environment where people with similar interests can transact (buy and sell goods); share interests, photos, videos; communicate with like-minded people; receive interest-related information; and even play out fantasies by adopting online personalities called avatars. Facebook, LinkedIn, Twitter, and Pinterest, and hundreds of other smaller, niche social networks all offer users community-building tools and services.

The basic value proposition of community providers is to create a fast, convenient, one-stop site where users can focus on their most important concerns and interests, share the experience with friends, and learn more about their own interests. Community providers typically rely on a hybrid revenue model that includes subscription fees, sales revenues, transaction fees, affiliate fees, and advertising fees from other firms that are attracted by a tightly focused audience.

Community providers make money from advertising and through affiliate relationships with retailers. Some of the oldest online communities are The Well, which provides a forum for technology and Internet-related discussions, and The Motley Fool, which provides financial advice, news, and opinions. The Well offers various membership plans ranging from \$10 to \$15 a month. Motley Fool supports itself through ads and selling products that start out “free” but turn into annual subscriptions.

Consumers' interest in communities is mushrooming. Community is, arguably, the fastest growing online activity. While many community providers have had a difficult time becoming profitable, many have succeeded over time, with advertising as their main source of revenue. Both the very large social networks such as Facebook, Twitter, and LinkedIn, as well as niche social networks with smaller dedicated audiences, are ideal marketing and advertising territories. Traditional online communities such as The Motley Fool and WebMD (which provides medical information to members) find that the breadth and depth of knowledge offered is an important factor. Community members frequently request knowledge, guidance, and advice. Lack of experienced

personnel can severely hamper the growth of a community, which needs facilitators and managers to keep discussions on course and relevant. For the newer community social networks, the most important ingredients of success appear to be ease and flexibility of use, and a strong customer value proposition. For instance, Facebook leapfrogged over its rival MySpace by encouraging the development of third-party revenue-producing applications.

Online communities benefit significantly from offline word-of-mouth, viral marketing. Online communities tend to reflect offline relationships. When your friends say they have a profile on Facebook, and ask you to “friend” them, you are encouraged to build your own online profile.

3 CONTENT PROVIDER

Content providers distribute information content, such as digital video, music, photos, text, and artwork. It is estimated that U.S. consumers will spend more than \$23 billion for online content such as movies, music, videos, television shows, e-books, and newspapers during 2016.

Content providers can make money via a variety of different revenue models, including advertising, subscription fees, and sales of digital goods. For instance, in the case of Apple Music, a monthly subscription fee provides users with access to millions of music tracks. Other content providers, such as the Wall Street Journal online newspaper, Harvard Business Review, and many others, charge customers for content downloads in addition to, or in place of, a subscription fee.

Of course, not all online content providers charge for their information: just look at the websites or mobile apps for ESPN, CIO, CNN, and the online versions of many newspapers and magazines. Users can access news and information without paying a cent, although sometimes they may be required to register as a member. These popular online content providers make money in other ways, such as through advertising and partner promotions. Increasingly, however, “free content” may be limited to headlines and text, whereas premium content—in-depth articles or videos—is sold for a fee.

Generally, the key to becoming a successful content provider is owning the content. Traditional owners of copyrighted content—publishers of books and newspapers, broadcasters of radio and television content, music publishers, and movie studios—have powerful advantages over newcomers who simply offer distribution channels and must pay for content, often at very high prices.

Some content providers, however, do not own content, but syndicate (aggregate) and then distribute content produced by others. Syndication is a major variation of the standard content provider model. Aggregators, who collect information from a wide variety of sources and then add value to that information through post-aggregation services, are another variation. For instance, Shopzilla collects information on the prices of thousands of goods online, analyzes the information, and presents users with tables showing the range of prices and links to the sites where the products can be purchased. Shopzilla adds value to content it aggregates, and resells this value to advertisers.

Any e-commerce start-up that intends to make money by providing content is likely to face difficulties unless it has a unique information source that others cannot

content provider

distributes information content, such as digital news, music, photos, video, and artwork

access. For the most part, this business category is dominated by traditional content providers. The *Insight on Technology* case, *Will the Connected Car Become the Next Hot Entertainment Vehicle?*, discusses how changes in Internet technology are driving the development of new business models in the online content market.

Online content is discussed in further depth in Chapter 10.

4

PORTAL

A gateway to Internet

portal

offers users powerful search tools as well as an integrated package of content and services all in one place

Portals such as Yahoo, MSN, and AOL offer users powerful search tools as well as an integrated package of content and services, such as news, e-mail, instant messaging, calendars, shopping, music downloads, video streaming, and more, all in one place. Initially, portals sought to be viewed as “gateways” to the Internet. Today, however, the portal business model is to be a destination. They are marketed as places where consumers will hopefully stay a long time to read news, find entertainment, and meet other people (think of destination resorts). Portals do not sell anything directly—or so it seems—and in that sense they can present themselves as unbiased. The market opportunity is very large: in 2016, around 265 million people in the United States accessed the Internet via a variety of devices at work or home. Portals generate revenue primarily by charging advertisers for ad placement, collecting referral fees for steering customers to other sites, and charging for premium services.

Although there are numerous portals/search engines, the top five (Google, Microsoft’s Bing, Yahoo, Ask, and AOL) gather more than 95% of the search engine traffic because of their superior brand recognition. Many of the top portal/search engines were among the first to appear on the Web and therefore had first-mover advantages. Being first confers advantage because customers come to trust a reliable provider and experience switching costs if they change to late arrivals in the market. By garnering a large chunk of the marketplace, first movers—just like a single telephone network—can offer customers access to commonly shared ideas, standards, and experiences (something called *network externalities* that we describe in later chapters).

The traditional portals have company: Facebook and other social networks are now the initial start or home page (portal) for millions of Internet users in the United States.

General and Specialized Portals

Yahoo, AOL, and others like them are considered to be horizontal portals because they define their marketplace to include all users of the Internet. Vertical portals (sometimes called vortals) attempt to provide similar services as horizontal portals, but are focused around a particular subject matter or market segment. For instance, Sailnet specializes in the consumer sailboat market that contains about 8 million Americans who own or rent sailboats. Although the total number of vortal users may be much lower than the number of portal users, if the market segment is attractive enough, advertisers are willing to pay a premium in order to reach a targeted audience. Also, visitors to specialized niche vortals spend more money than the average Yahoo visitor. Google and Ask can also be considered portals of a sort, but focus primarily on offering search and advertising services. They generate revenues primarily from search engine advertising sales and also from affiliate referral fees.

INSIGHT ON TECHNOLOGY

WILL THE CONNECTED CAR BECOME THE NEXT HOT ENTERTAINMENT VEHICLE?

You're in the driver's seat of your car, commuting to work. But instead of keeping your eyes on the road, you're watching a Netflix movie, logging on to Facebook, and checking your e-mail. And no, you are not an accident waiting to happen.

This scenario is one that is likely to become commonplace in the not too distant future. In 2016, we are on the cusp of yet another revolution in the way we live our lives, this time driven by technology known as the Internet of Things (IoT). IoT refers to the use of sensors connected to the Internet and cloud computers, coupled with powerful data analytics programs, to track things and make sense out of their behavior (you'll learn more about IoT in Chapter 3). The technology behind IoT already exists, and now businesses are working on using it to develop products and services that consumers and businesses are willing to pay for.

From a business perspective, IoT is not just a collection of technologies, but an enabler for services that can be sold to other businesses and consumers. For businesses, IoT may mean more effective and efficient maintenance, remote monitoring of equipment, tracking assets in the supply chain, and identifying patterns of behavior of machines and operators. These services translate into cost reduction, and greater profits for firms that truly understand IoT. For consumers, IoT means self-driving smart cars, intelligent media systems, smart homes, personal health monitoring, and retail and e-commerce automation.

Gartner estimates that 6.4 billion connected things are in use worldwide in 2016, 5.5 million new things are added every day, and over 20 billion will be connected by 2020. McKinsey estimates

that IoT will produce from \$4 to \$11 trillion in value by 2025, with 70% of this value occurring in B2B commerce, and the rest in B2C commerce. For suppliers of IoT hardware, software, and telecommunications, it's a bonanza of potential sales revenue. Along the way, IoT is going to transform business processes and enable a host of new business models in a variety of different industries.

One arena that IoT is expected to have a significant impact on is the content industry, especially when coupled with its increasing use in the automobile industry to create connected, and ultimately, self-driving cars that will free drivers from having to focus on the road. Today, your car is still probably one of the least connected devices in your digital life, but that is rapidly changing, in part due to consumer demand. A recent survey found that almost two-thirds of U.S. car owners with broadband Internet access in their homes wanted similar access in their cars. A connected car is equipped with hundreds of sensors and has direct access to the Internet, as well as links to hundreds of other connected objects. Tiny sensors will be able to report on your route and destination, the state of your tires, air conditioning, what music you are listening to, and in the future, perhaps even your state of mind, using sentiment sensors that can pick up anger, tears, crying, and laughing.

The number of connected cars on the road is rapidly increasing. According to one industry analysis, more than 40 million cars in the United States were already connected to the Internet by the beginning of 2016. Telecommunications companies are, not surprisingly, very interested in connected cars as platforms for their services and are facilitating their development. AT&T, for example, introduced an expanded connected car platform in

(continued)

2016, which allows unlimited plan smartphone customers to add their car to the service for \$40 a month, or \$10 a month for 1 gigabyte of data. In 2016, AT&T also signed an agreement with Ford to connect 10 million Ford cars using Ford's new SYNC Connect system. AT&T is also working with a number of other auto companies to install wireless access devices in cars. Aside from selling its wireless network to consumers, AT&T is planning to sell data collected from cars and drivers that will allow ads to be targeted, based on car model, locations, and even the kind of music listened to.

For content distributors, IoT offers a whole new venue. Connected cars provide a potentially huge market for media companies. People (drivers and passengers) spend about 500 hours in a vehicle per year, including 42 hours in traffic. This captive audience is an ideal target for both marketers and media companies. Today, although we primarily think of cars as transportation, they are also entertainment and media centers. For instance, cars are already the main source of radio revenues in the United States, with more than half of all radio consumption taking place in a car. But using online radio services in today's cars is most often a painful process that often fails to work properly. Both carmakers and content providers have been hard at work fixing this problem. Pandora Media, seeking to build on its existing dominance in the online radio market, has entered into agreements with 24 auto brands to embed its music service into over 160 car models. Spotify,

Apple's CarPlay, and Google's Android Auto also have new services for connected cars. Cars will eventually become like a mobile living room, with video services that deliver ads along with movies and TV shows (currently, for the rear seats only, but moving to the front seats in a self-driving car). As cars become more and more automated and drivers are able to shift from driving to watching video content, consulting firm EY estimates that video industry revenue may increase by more than \$20 billion. Connected cars are also likely to feature enhanced dashboard interfaces that will enable easy access to email, music streaming, and social networks.

In addition to changing the type of content available in automobiles, IoT is also expected to have the ability to deliver much more personalized content. IoT sensors will make it possible for sensors to recognize individual consumers and offer suggested content on the basis of their past behavior and preferences. Advertisers are already imagining ways to use the shape of a car to create immersive, 360-degree ad experiences. To that end, Ford patented a driverless car windshield entertainment system that could be the basis for this type of advertising as well as consuming traditional video content. Other forms of personalization could include the ability to find the nearest available parking place, locating nearby favorite restaurants or other attractions, and the ability to take your "driving profile" with you from car to car, including preferences and tendencies.

SOURCES: "5 Reasons the Music Industry Should Care About Driverless Cars," by Cherie Hu, Hypebot.com, October 26, 2016; "Detroit's Music Chops and Auto Shops Could Drive Connected-Car Entertainment," by Scott Keeney, Techcrunch.com, August 30, 2016; "The Internet of Things Is Here, and It Isn't a Thing," by Christopher Mims, *Wall Street Journal*, August 21, 2016; "DASH Podcast Episode 7: Audio Entertainment in Self-Driving Cars (Andreas Mail)," by Seth Resler, Jacobsmedia.com, August 17, 2016; "Will IoT Totally Reshape How, When, and Where We Get Content," by Chris Gianutsos, Readwrite.com, July 8, 2016; "Verizon Acquisition of Telogis Expands Company's Connected Car Footprint," by Doug Newcomb, Forbes.com, June 30, 2016; "Media and Entertainment Meet the Internet of Things," by Chase Martin, Mediapost.com, June 22, 2016; "The Connected Car Report: Forecasts, Competing Technologies, and Leading Manufacturers," by John Greenough, BusinessInsider.com, June 10, 2016; "The Internet of Things," by Victoria Petrock, eMarketer, Inc., May 2016; "AT&T Just Took a Big Step to Maintain Its Lead in Wireless Service for Connected Cars," by Andrew Meola, Businessinsider.com, May 23, 2016; "How Ford Is Building the Connected Car," by Steven Norton, *Wall Street Journal*, February 21, 2016; "The Internet of Media and Entertainment Things," by Victoria Petrock, eMarketer, Inc., February 2016; "The Internet of Automotive Things," by Victoria Petrock, eMarketer, Inc., February 2016; "The Top Five Trends for the Connected Car in 2016," by Mahbulul Alam, Techcrunch.com, January 2, 2016; "AT&T and the Connected Car Making Cars Smarter and Safer," Business.att.com, 2016; "State of the Market: Internet of Things 2016," by Verizon, 2016; "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015," Gartner.com, November 10, 2015; "The Internet of Things: Mapping the Value Beyond the Hype," McKinsey & Company, June 2015.

5 TRANSACTION BROKER

Companies that process transactions for consumers normally handled in person, by phone, or by mail are **transaction brokers**. The largest industries using this model are financial services, travel services, and job placement services. The online transaction broker's primary value propositions are savings of money and time. In addition, most transaction brokers provide timely information and opinions. Companies such as Monster offer job searchers a national marketplace for their talents and employers a national resource for that talent. Both employers and job seekers are attracted by the convenience and currency of information. Online stock brokers charge commissions that are considerably less than traditional brokers, with many offering substantial deals, such as cash and a certain number of free trades, to lure new customers.

Given rising consumer interest in financial planning and the stock market, the market opportunity for online transaction brokers appears to be large. However, while millions of customers have shifted to online brokers, some are still wary about switching from their traditional broker who provides personal advice and a brand name. Fears of privacy invasion and the loss of control over personal financial information also contribute to market resistance. Consequently, the challenge for online brokers is to overcome consumer fears by emphasizing the security and privacy measures in place, and, like physical banks and brokerage firms, providing a broad range of financial services and not just stock trading. This industry is covered in greater depth in Chapter 9.

Transaction brokers make money each time a transaction occurs. Each stock trade, for example, nets the company a fee, based on either a flat rate or a sliding scale related to the size of the transaction. Attracting new customers and encouraging them to trade frequently are the keys to generating more revenue for these companies. Travel sites generate commissions from travel bookings and job sites generate listing fees from employers up front, rather than charging a fee when a position is filled.

transaction broker

processes transactions for consumers that are normally handled in person, by phone, or by mail

6 MARKET CREATOR

Market creators build a digital environment in which buyers and sellers can meet, display and search for products and services, and establish prices. Prior to the Internet and the Web, market creators relied on physical places to establish a market. Beginning with the medieval marketplace and extending to today's New York Stock Exchange, a market has meant a physical space for transacting business. There were few private digital network marketplaces prior to the Web. The Web changed this by making it possible to separate markets from physical space. Prime examples are Priceline, which allows consumers to set the price they are willing to pay for various travel accommodations and other products (sometimes referred to as a reverse auction), and eBay, the online auction site utilized by both businesses and consumers. Market creators make money by either charging a percentage of every transaction made, or charging merchants for access to the market.

For example, eBay's auction business model is to create a digital environment for buyers and sellers to meet, agree on a price, and transact. This is different from transaction brokers who actually carry out the transaction for their customers, acting as agents in larger markets. At eBay, the buyers and sellers are their own agents. Each

market creator

builds a digital environment where buyers and sellers can meet, display products, search for products, and establish a price for products

sale on eBay nets the company a commission based on the percentage of the item's sales price, in addition to a listing fee. eBay is one of the few e-commerce companies that has been profitable virtually from the beginning. Why? One answer is that eBay has no inventory or production costs. It is simply a middleman.

The market opportunity for market creators is potentially vast, but only if the firm has the financial resources and marketing plan to attract sufficient sellers and buyers to the marketplace. As of June 30, 2016, eBay had more than 164 million active buyers, and this makes for an efficient market (eBay Inc., 2016). There are many sellers and buyers for each type of product, sometimes for the same product, for example, laptop computer models. Many other digital auctions have sprung up in smaller, more specialized vertical market segments such as jewelry and automobiles.

Uber, Airbnb, and Lyft are another example of the market creator business model (although they could also be categorized as service providers). On-demand service companies (also sometimes called sharing economy companies) are market creators that have developed online platforms that allow people to sell services, such as transportation or spare rooms, in a marketplace that operates in the cloud and relies on the Web or smartphone apps to conduct transactions. It is important to note that, although referred to as sharing economy or mesh economy companies, these companies do not in fact share resources. Users of these services are either selling something or buying something, and the companies produce revenue by extracting fees for each transaction. However, they do unlock the economic value in spare resources (personal cars and rooms) that might otherwise have been lost. In the process they have created huge online markets. For instance, Uber (founded in 2009) currently operates in over 480 cities in 69 countries around the world. Airbnb, founded in 2008, operates in more than 190 countries and 34,000 cities, lists over 2 million rooms available for rent, and has had over 60 million people use its services to book a room. Airbnb has raised around \$2.4 billion in funding thus far and is valued at \$30 billion; Uber has raised over \$12.5 billion and is valued at around \$68 billion.

7

SERVICE PROVIDER

service provider
offers services online

While e-tailers sell products online, **service providers** offer services online. There's been an explosion in online services that is often unrecognized. Photo sharing, video sharing, and user-generated content (in blogs and social networks) are all services provided to customers. Google has led the way in developing online applications such as Google Maps, Google Docs, and Gmail. Other personal services such as online medical bill management, financial and pension planning, and travel recommendation are showing strong growth.

Service providers use a variety of revenue models. Some charge a fee, or monthly subscriptions, while others generate revenue from other sources, such as through advertising and by collecting personal information that is useful in direct marketing. Many service providers employ a freemium revenue model, in which some basic services are free, but others require the payment of additional charges. Much like retailers who trade products for cash, service providers trade knowledge, expertise, and capabilities for revenue.

Obviously, some services cannot be provided online. For example, dentistry, plumbing, and car repair cannot be completed via the Internet. However, online arrangements can be made for these services. Online service providers may offer computer services, such as data storage (Dropbox and Carbonite), provide legal services (RocketLawyer), or accounting or bookkeeping services (Wave, Bench). Grocery shopping sites such as FreshDirect and Peapod are also providing services.¹ To complicate matters a bit, most financial transaction brokers (described previously) provide services such as college tuition and pension planning. Travel brokers also provide vacation-planning services, not just transactions with airlines and hotels. Indeed, mixing services with your products is a powerful business strategy pursued by many hard-goods companies (for example, warranties are services).

The basic value proposition of service providers is that they offer consumers valuable, convenient, time-saving, and low-cost alternatives to traditional service providers or provide services that are truly unique. Where else can you search billions of web pages, or share photos with as many people instantly? Research has found, for instance, that a major factor in predicting online buying behavior is *time starvation*. Time-starved people tend to be busy professionals who work long hours and simply do not have the time to pick up packages, buy groceries, send photos, or visit with financial planners (Bellman, Lohse, and Johnson, 1999). The market opportunity for service providers is as large as the variety of services that can be provided and potentially is much larger than the market opportunity for physical goods. We live in a service-based economy and society; witness the growth of fast-food restaurants, package delivery services, and wireless cellular phone services. Consumers' increasing demand for convenience products and services bodes well for current and future online service providers.

Marketing of service providers must allay consumer fears about hiring a vendor online, as well as build confidence and familiarity among current and potential customers. Building confidence and trust is critical for service providers just as it is for retail product merchants.

2.3 MAJOR BUSINESS-TO-BUSINESS (B2B) BUSINESS MODELS

In Chapter 1, we noted that business-to-business (B2B) e-commerce, in which businesses sell to other businesses, is more than 10 times the size of B2C e-commerce, even though most of the public attention has focused on B2C. For instance, it is estimated that revenues for all types of B2B e-commerce in the United States will total around \$6.7 trillion in 2016, compared to about \$600 billion for all types of B2C e-commerce. Clearly, most of the dollar revenues in e-commerce involve B2B e-commerce.

¹ FreshDirect and other e-commerce businesses can also be classified as online retailers insofar as they warehouse commonly purchased items and make a profit based on the spread between their buy and sell prices.

TABLE 2.7 B2B BUSINESS MODELS			
BUSINESS MODEL	EXAMPLES	DESCRIPTION	REVENUE MODEL
<i>(1) NET MARKETPLACE</i>			
E-distributor	Grainger Amazon Business	Single-firm online version of retail and wholesale store; supply maintenance, repair, operation goods; indirect inputs	Sales of goods
E-procurement	Ariba Supplier Network PerfectCommerce	Single firm creating digital markets where sellers and buyers transact for indirect inputs	Fees for market-making services, supply chain management, and fulfillment services
Exchange	Go2Paper	Independently owned vertical digital marketplace for direct inputs	Fees and commissions on transactions
Industry Consortium	TheSeam SupplyOn	Industry-owned vertical digital market open to select suppliers	Fees and commissions on transactions
<i>(2) PRIVATE INDUSTRIAL NETWORK</i>			
	Walmart Procter & Gamble	Company-owned network that coordinates supply chains with a limited set of partners	Cost absorbed by network owner and recovered through production and distribution efficiencies

Much of this activity is unseen and unknown to the average consumer. **Table 2.7** lists the major business models utilized in the B2B arena.

1

E-DISTRIBUTOR

e-distributor

a company that supplies products and services directly to individual businesses

Revenue model:
sales of goods

Companies that supply products and services directly to individual businesses are **e-distributors**. W.W. Grainger, for example, is the largest distributor of maintenance, repair, and operations (MRO) supplies. In the past, Grainger relied on catalog sales and physical distribution centers in metropolitan areas. Its catalog of equipment went online in 1995. In 2015, Grainger's e-commerce platform, which includes websites and mobile apps, produced \$3.3 billion in sales (41% of its total revenue) for the company.

E-distributors are owned by one company seeking to serve many customers. However, as with exchanges (described on the next page), critical mass is a factor. With e-distributors, the more products and services a company makes available, the more attractive it is to potential customers. One-stop shopping is always preferable to having to visit numerous sites to locate a particular part or product.

2

E-PROCUREMENT

e-procurement firm creates and sells access to digital markets

Just as e-distributors provide products to other companies, **e-procurement firms** create and sell access to digital markets. Firms such as Ariba, for instance, have created software that helps large firms organize their procurement process by creating mini-digital markets for a single firm. Ariba creates custom-integrated online catalogs

(where supplier firms can list their offerings) for purchasing firms. On the sell side, Ariba helps vendors sell to large purchasers by providing software to handle catalog creation, shipping, insurance, and finance. Both the buy and sell side software is referred to generically as “value chain management” software.

B2B service providers make money through transaction fees, fees based on the number of workstations using the service, or annual licensing fees. They offer purchasing firms a sophisticated set of sourcing and supply chain management tools that permit firms to reduce supply chain costs. In the software world, firms such as Ariba are sometimes also called Software as a Service (SaaS) or Platform as a Service (PaaS) providers; they are able to offer firms much lower costs of software by achieving scale economies. **Scale economies** are efficiencies that result from increasing the size of a business, for instance, when large, fixed-cost production systems (such as factories or software systems) can be operated at full capacity with no idle time. In the case of software, the marginal cost of a digital copy of a software program is nearly zero, and finding additional buyers for an expensive software program is exceptionally profitable. This is much more efficient than having every firm build its own supply chain management system, and it permits firms such as Ariba to specialize and offer their software to firms at a cost far less than the cost of developing it.

3 EXCHANGES

Exchanges have garnered most of the B2B attention and early funding because of their potential market size even though today they are a small part of the overall B2B picture. An **exchange** is an independent digital marketplace where hundreds of suppliers meet a smaller number of very large commercial purchasers (Kaplan and Sawhney, 2000). Exchanges are owned by independent, usually entrepreneurial start-up firms whose business is making a market, and they generate revenue by charging a commission or fee based on the size of the transactions conducted among trading parties. They usually serve a single vertical industry such as steel, polymers, or aluminum, and focus on the exchange of direct inputs to production and short-term contracts or spot purchasing. For buyers, B2B exchanges make it possible to gather information, check out suppliers, collect prices, and keep up to date on the latest happenings all in one place. Sellers, on the other hand, benefit from expanded access to buyers. The greater the number of sellers and buyers, the lower the sales cost and the higher the chances of making a sale. The ease, speed, and volume of transactions are summarily referred to as *market liquidity*.

In theory, exchanges make it significantly less expensive and time-consuming to identify potential suppliers, customers, and partners, and to do business with each other. As a result, they can lower transaction costs—the cost of making a sale or purchase. Exchanges can also lower product costs and inventory-carrying costs—the cost of keeping a product on hand in a warehouse. In reality, as will be discussed in Chapter 12, B2B exchanges have had a difficult time convincing thousands of suppliers to move into singular digital markets where they face powerful price competition, and an equally difficult time convincing businesses to change their purchasing behavior away from trusted long-term trading partners. As a result, the number of exchanges has fallen significantly.

value chain: a strategy development tool which is a way to think about designing:

- what your company does and does not focus on
- what is important for customers
- what creates sustainable competitive advantages

B2B service provider

sells business services to other firms

scale economies

efficiencies that arise from increasing the size of a business

e-procurement is a tool that enable procurement activities including:

- sourcing
- ordering
- commissioning
- receipting and making payment

exchange

an independent digital marketplace where suppliers and commercial purchasers can conduct transactions

4 INDUSTRY CONSORTIA

industry consortia

industry-owned vertical marketplaces that serve specific industries

Industry consortia are industry-owned *vertical marketplaces* that serve specific industries, such as the automobile, aerospace, chemical, floral, or logging industries. In contrast, *horizontal marketplaces* sell specific products and services to a wide range of companies. *Vertical marketplaces* supply a smaller number of companies with products and services of specific interest to their industry, while *horizontal marketplaces* supply companies in different industries with a particular type of product and service, such as marketing-related, financial, or computing services. For example, SupplyOn, founded in 2000 and owned by industrial giants Bosch (one of the world's largest suppliers of automotive components), Continental (a leading automotive manufacturing company), and Schaeffler (a global manufacturer of various types of bearings), among others, provides a shared supply chain collaboration platform for companies in various manufacturing industries. In 2016, in addition to its shareholders, its customers include Airbus, BMW, BorgWarner, Siemens, Thales, and many other major global manufacturing companies.

Industry consortia have tended to be more successful than independent exchanges in part because they are sponsored by powerful, deep-pocketed industry players, and also because they strengthen traditional purchasing behavior rather than seek to transform it.

5 PRIVATE INDUSTRIAL NETWORKS

private industrial network

digital network designed to coordinate the flow of communications among firms engaged in business together

A **private industrial network** (sometimes referred to as a private trading exchange or PTX) is a digital network designed to coordinate the flow of communications among firms engaged in business together. The network is owned by a single large purchasing firm. Participation is by invitation only to trusted long-term suppliers of direct inputs. These networks typically evolve out of a firm's own enterprise resource planning (ERP) system, and are an effort to include key suppliers in the firm's own business decision making. For instance, Walmart operates one of the largest private industrial networks in the world for its suppliers, who on a daily basis use Walmart's network to monitor the sales of their goods, the status of shipments, and the actual inventory level of their goods.

We discuss the nuances of B2B e-commerce in more detail in Chapter 12.

2.4 HOW E-COMMERCE CHANGES BUSINESS: STRATEGY, STRUCTURE, AND PROCESS

Now that you have a clear grasp of the variety of business models used by e-commerce firms, you also need to understand how e-commerce has changed the business environment in the last decade, including *industry structures*, *business strategies*, and *industry and firm operations* (business processes and value chains). We return to these concepts throughout the book as we explore the *e-commerce phenomenon*. In general, the Internet is an open standards system available to all players, and this fact inherently makes it easy for new competitors to enter the marketplace and offer substitute

TABLE 2.8

EIGHT UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY

FEATURE	SELECTED IMPACTS ON BUSINESS ENVIRONMENT
Ubiquity	Alters industry structure by <u>creating new marketing channels and expanding size of overall market</u> . Creates new efficiencies in industry operations and lowers costs of firms' sales operations. Enables new <u>differentiation strategies</u> .
Global reach	Changes industry structure by <u>lowering barriers to entry</u> , but greatly expands market at the same time. Lowers cost of industry and firm operations through <u>production and sales efficiencies</u> . Enables <u>competition on a global scale</u> .
Universal standards	Changes industry structure by <u>lowering barriers to entry and intensifying competition within an industry</u> . Lowers costs of industry and firm operations by <u>lowering computing and communications costs</u> . Enables <u>broad scope strategies</u> .
Richness	Alters industry structure by <u>reducing strength of powerful distribution channels</u> . Changes industry and firm operations costs by <u>reducing reliance on sales forces</u> . Enhances post-sales support strategies.
Interactivity	Alters industry structure by <u>reducing threat of substitutes through enhanced customization</u> . Reduces industry and firm costs by <u>reducing reliance on sales forces</u> . Enables <u>differentiation strategies</u> .
Personalization/ Customization	Alters industry structure by <u>reducing threats of substitutes, raising barriers to entry</u> . Reduces value chain costs in industry and firms by <u>lessening reliance on sales forces</u> . Enables <u>personalized marketing strategies</u> .
Information density	Changes industry structure by <u>weakening powerful sales channels, shifting bargaining power to consumers</u> . Reduces industry and firm operations costs by <u>lowering costs of obtaining, processing, and distributing information about suppliers and consumers</u> .
Social technologies	Changes industry structure by shifting programming and editorial decisions to consumers. Creates substitute entertainment products. Energizes a large group of new suppliers.

products or channels of delivery. The Internet tends to intensify competition. Because information becomes available to everyone, the Internet inherently shifts power to buyers who can quickly discover the lowest-cost provider. On the other hand, the Internet presents many new opportunities for creating value, for branding products and charging premium prices, and for enlarging an already powerful offline physical business such as Walmart or Sears.

Recall Table 1.2 in Chapter 1 that describes the truly unique features of e-commerce technology. **Table 2.8** suggests some of the implications of each unique feature for the overall business environment—industry structure, business strategies, and operations.

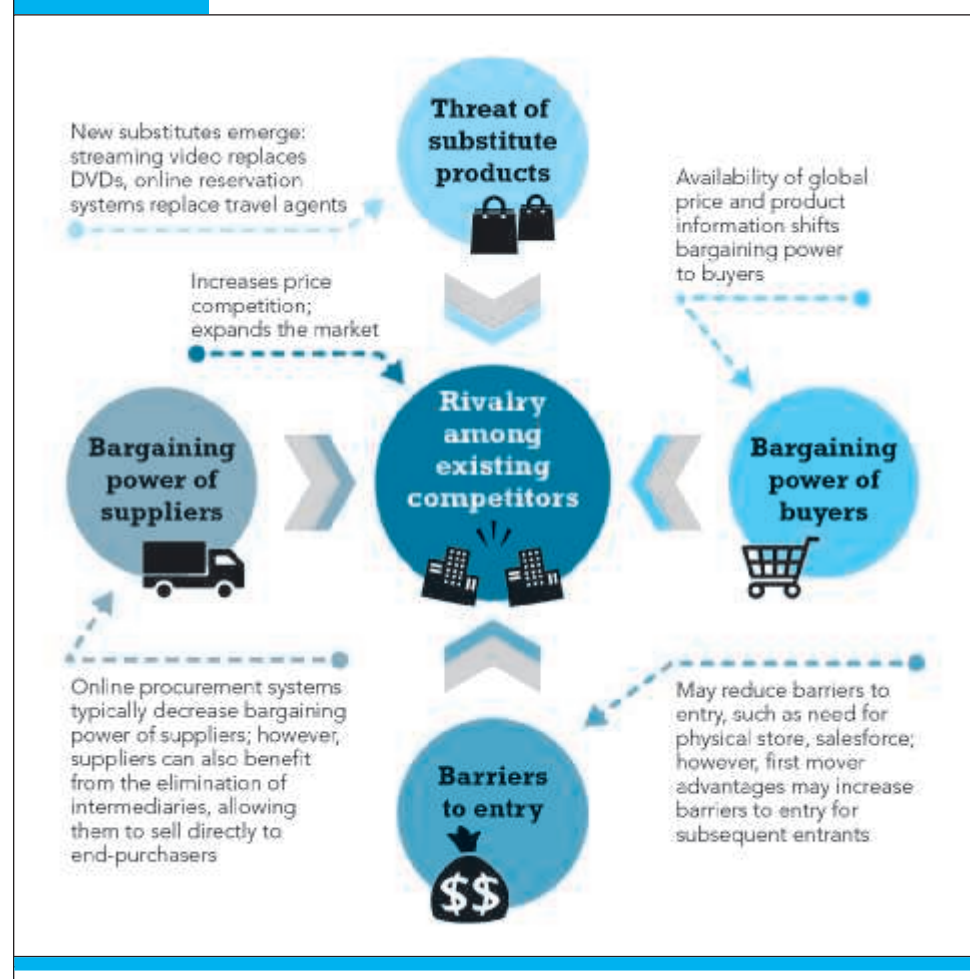
industry structure refers to the nature of the players in an industry and their relative bargaining power

INDUSTRY STRUCTURE

E-commerce changes industry structure, in some industries more than others. **Industry structure** refers to the nature of the players in an industry and their relative bargaining power. An industry's structure is characterized by five forces: *rivalry among existing competitors*, the *threat of substitute products*, *barriers to entry into the industry*, the *bargaining power of suppliers*, and the *bargaining power of buyers* (Porter, 1985). When you describe an industry's structure, you are describing the **general business environment** in an industry and the **overall profitability of doing business** in that environment. E-commerce has the potential to change the relative strength of these competitive forces (see Figure 2.3).

FIGURE 2.3

HOW E-COMMERCE INFLUENCES INDUSTRY STRUCTURE



E-commerce has many impacts on industry structure and competitive conditions. From the perspective of a single firm, these changes can have negative or positive implications depending on the situation. In some cases, an entire industry can be disrupted, while at the same time, a new industry is born. Individual firms can either prosper or be devastated.

When you consider a business model and its potential long-term profitability, you should always perform an industry structural analysis. An **industry structural analysis** is an effort to understand and describe the nature of competition in an industry, the nature of substitute products, the barriers to entry, and the relative strength of consumers and suppliers.

E-commerce can affect the structure and dynamics of industries in very different ways. Consider the **recorded music industry**, an industry that has experienced significant change because of e-commerce. Historically, the major record companies owned the exclusive rights to the recorded music of various artists. With the entrance into the marketplace of substitute providers such as **Napster** and **Kazaa**, millions of consumers began to use the Internet to bypass traditional music labels and their distributors entirely. In the **travel industry**, entirely new middlemen such as **Travelocity** entered the market to compete with traditional travel agents. After **Travelocity**, **Expedia**, **CheapTickets**, and other travel services demonstrated the power of e-commerce marketing for airline tickets, the actual owners of the airline seats—the major airlines—banded together to form their own Internet outlet for tickets, **Orbitz**, for direct sales to consumers (although ultimately selling the company to a private investor group). Clearly, e-commerce creates *new industry dynamics* that can best be described as the give and take of the marketplace, the changing fortunes of competitors.

Yet, in other industries, e-commerce has strengthened existing players. In the chemical and automobile industries, e-commerce is being used effectively by manufacturers to strengthen their traditional distributors. In these industries, e-commerce technology has not fundamentally altered the **competitive forces**—**bargaining power of suppliers**, **barriers to entry**, **bargaining power of buyers**, **threat of substitutes**, or **rivalry among competitors**—within the industry. Hence, each industry is different and you need to examine each one carefully to understand the impacts of e-commerce on competition and strategy.

New forms of distribution created by new market entrants can completely change the competitive forces in an industry. For instance, consumers gladly substituted free access to Wikipedia for a \$699 set of World Book encyclopedias, or a \$40 DVD, radically changing the competitive forces in the encyclopedia industry. As we describe in Chapter 10, the content industries of newspapers, books, movies, games, and television have been transformed by the emergence of new distribution platforms.

Inter-firm rivalry (competition) is one area of the business environment where e-commerce technologies have had an impact on most industries. In general, e-commerce has increased **price competition** in nearly all markets. It has been relatively easy for existing firms to adopt e-commerce technology and attempt to use it to achieve competitive advantage vis-à-vis rivals. For instance, e-commerce inherently changes the scope of competition from local and regional to national and global. Because consumers have access to global price information, e-commerce produces pressures on firms to compete by lowering prices (and lowering profits). On the other hand, e-commerce has made it possible for some firms **to differentiate their products or services from others**. **Amazon** patented one-click purchasing, for instance, while **eBay** created a unique, easy-to-use interface and a differentiating brand name. Therefore, although e-commerce has increased emphasis on price competition, it has also enabled businesses to create new strategies for differentiation and branding so that they can retain higher prices.

industry structural analysis

an effort to understand and describe the nature of competition in an industry, the nature of substitute products, the barriers to entry, and the relative strength of consumers and suppliers

threat of substitutes

competition in an industry

rivalry among competitors

1

2

bargaining power of buyers

bargaining power of suppliers

It is impossible to determine if e-commerce technologies have had an overall positive or negative impact on firm profitability in general. Each industry is unique, so it is necessary to perform a separate analysis for each one. Clearly, e-commerce has shaken the foundations of some industries, in particular, content industries (such as the music, newspaper, book, and software industries) as well as other information-intense industries such as financial services. In these industries, the power of consumers has grown relative to providers, prices have fallen, and overall profitability has been challenged. In other industries, especially manufacturing, e-commerce has not greatly changed relationships with buyers, but has changed relationships with suppliers. Increasingly, manufacturing firms in entire industries have banded together to aggregate purchases, create industry exchanges or marketplaces, and outsource industrial processes in order to obtain better prices from suppliers. Throughout this book, we document these changes in industry structure and market dynamics introduced by e-commerce.

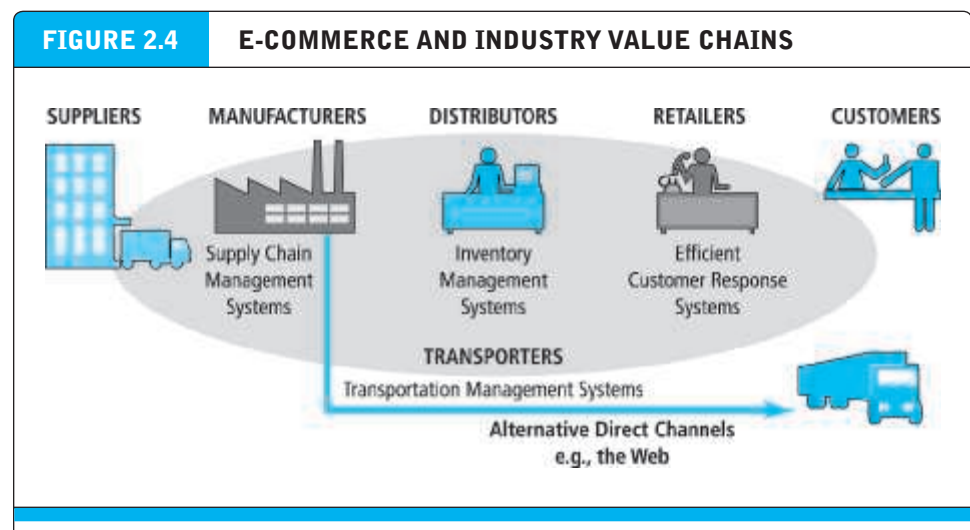
INDUSTRY VALUE CHAINS

The Analysis of value chain helps to understand the impact of EC on Business operations

value chain

the set of activities performed in an industry or in a firm that transforms raw inputs into final products and services

While an industry structural analysis helps you understand the impact of e-commerce technology on the overall business environment in an industry, a more detailed industry value chain analysis can help identify more precisely just how e-commerce may change business operations at the industry level. One of the basic tools for understanding the impact of information technology on industry and firm operations is the value chain. The concept is quite simple. A value chain is the set of activities performed in an industry or in a firm that transforms raw inputs into final products and services. Each of these activities adds economic value to the final product; hence, the term value chain as an interconnected set of value-adding activities. **Figure 2.4** illustrates the six generic players in an industry value chain: suppliers, manufacturers, transporters, distributors, retailers, and customers.



Every industry can be characterized by a set of value-adding activities performed by a variety of actors. E-commerce potentially affects the capabilities of each player as well as the overall operational efficiency of the industry.

By reducing the cost of information, e-commerce offers each of the key players in an industry value chain new opportunities to maximize their positions by lowering costs and/or raising prices. For instance, manufacturers can reduce the costs they pay for goods by developing Internet-based B2B exchanges with their suppliers. Manufacturers can develop direct relationships with their customers, bypassing the costs of distributors and retailers. Distributors can develop highly efficient inventory management systems to reduce their costs, and retailers can develop highly efficient customer relationship management systems to strengthen their service to customers. Customers in turn can search for the best quality, fastest delivery, and lowest prices, thereby lowering their transaction costs and reducing prices they pay for final goods. Finally, the operational efficiency of the entire industry can increase, lowering prices and adding value for consumers, and helping the industry to compete with alternative industries.

1

2

4

5

FIRM VALUE CHAINS

The concept of value chain can be used to analyze a single firm's operational efficiency as well. The question here is: How does e-commerce technology potentially affect the value chains of firms within an industry? A firm value chain is the set of activities a firm engages in to create final products from raw inputs. Each step in the process of production adds value to the final product. In addition, firms develop support activities that coordinate the production process and contribute to overall operational efficiency.

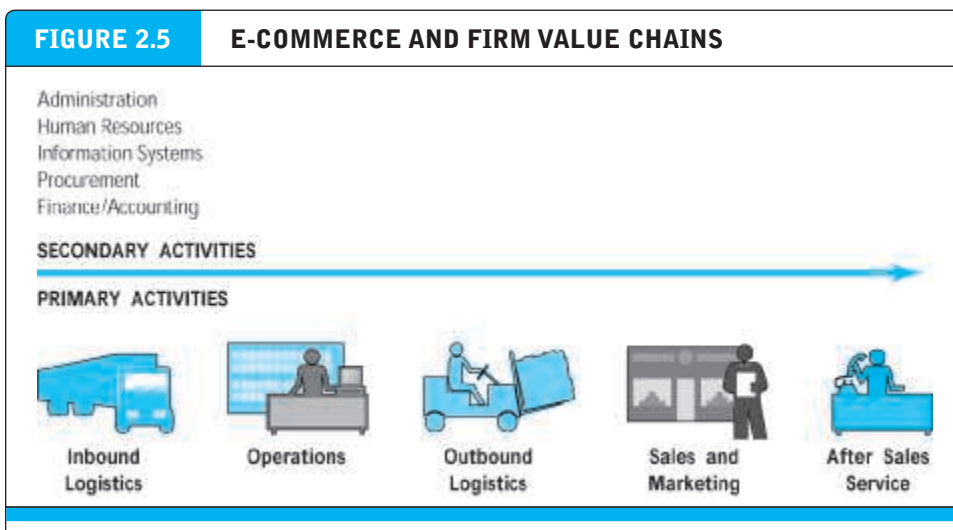
firm value chain

the set of activities a firm engages in to create final products from raw inputs

Figure 2.5 illustrates the key steps and support activities in a firm's value chain.

E-commerce offers firms many opportunities to increase their operational efficiency and differentiate their products. For instance, firms can use the Internet's communications efficiency to outsource some primary and secondary activities to specialized, more efficient providers without such outsourcing being visible to the

1



Porter's Value Chain
- Support Activities (Secondary Activities)
- Primary Activities

Inbound logistics: the process related to receiving, sorting, and distributing inputs.
Operations: the activities that change the inputs to outputs. here operational system create value.
Outbound logistics: the activities that deliver your products or services to your customers

Every firm can be characterized by a set of value-adding primary and secondary activities performed by a variety of actors in the firm. A simple firm value chain performs five primary value-adding steps: inbound logistics, operations, outbound logistics, sales and marketing, and after sales service.

2

consumer. In addition, firms can use e-commerce to more precisely coordinate the steps in the value chains and reduce their costs. Finally, firms can use e-commerce to provide users with more differentiated and high-value products. For instance, Amazon provides consumers with a much larger inventory of books to choose from, at a lower cost, than traditional book stores. It also provides many services—such as instantly available professional and consumer reviews, and information on buying patterns of other consumers—that traditional bookstores cannot.

3

FIRM VALUE WEBS

While firms produce value through their value chains, they also rely on the value chains of their partners—their suppliers, distributors, and delivery firms. E-commerce creates new opportunities for firms to cooperate and create a value web. A value web is a networked business ecosystem that uses e-commerce technology to coordinate the value chains of business partners within an industry, or at the first level, to coordinate the value chains of a group of firms. Figure 2.6 illustrates a value web.

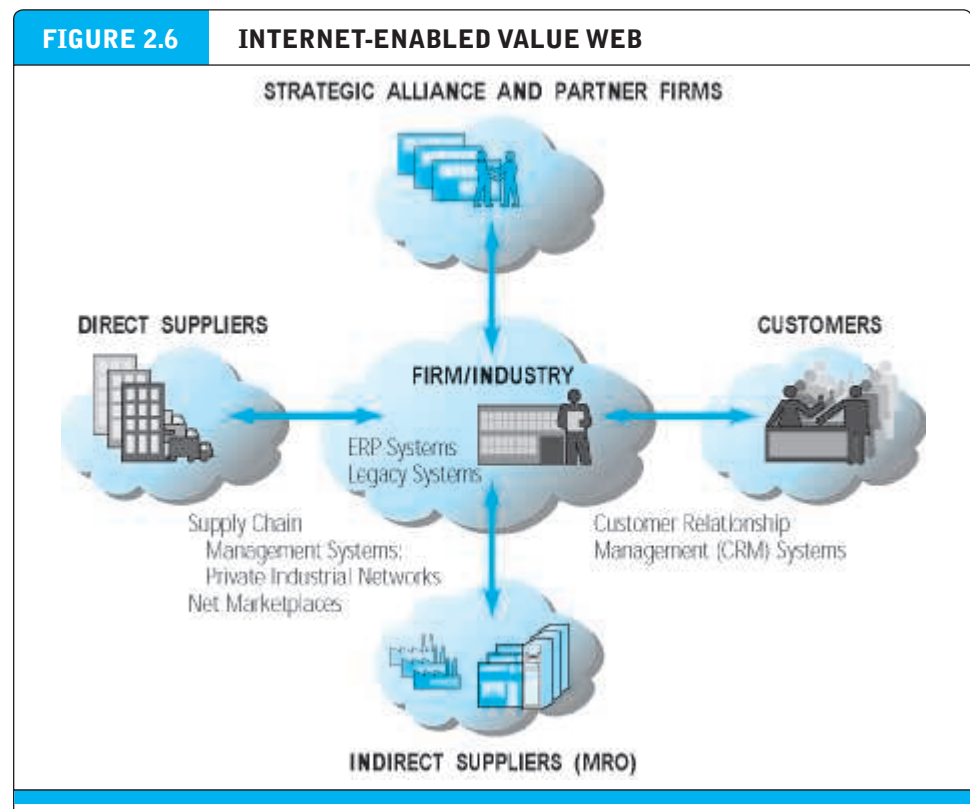
A value web coordinates a firm's suppliers with its own production needs using an Internet-based supply chain management system. We discuss these B2B systems

value web

networked business ecosystem that coordinates the value chains of several firms

ERP : Enterprise Resource Planning which is a tool to manage information.

Information Management is the organized collection, storage and use of information for the benefit of an enterprise.



Internet technology enables firms to create an enhanced value web in cooperation with their strategic alliance and partner firms, customers, and direct and indirect suppliers.

in Chapter 12. Firms also use the Internet to develop close relationships with their logistics partners. For instance, Amazon relies on UPS tracking systems to provide its customers with online package tracking, and it relies on the U.S. Postal Service systems to insert packages directly into the mail stream. Amazon has partnership relations with hundreds of firms to generate customers and to manage relationships with customers. In fact, when you examine Amazon closely, you realize that the value it delivers to customers is in large part the result of coordination with other firms and not simply the result of activities internal to Amazon. The value of Amazon is, in large part, the value delivered by its value web partners. This is difficult for other firms to imitate in the short run.

BUSINESS STRATEGY

A **business strategy** is a set of plans for achieving superior long-term returns on the capital invested in a business firm. A business strategy is therefore a plan for making profits in a competitive environment over the long term. **Profit** is simply the difference between the price a firm is able to charge for its products and the cost of producing and distributing goods. Profit represents **economic value**. **Economic value** is created anytime customers are willing to pay more for a product than it costs to produce. Why would anyone pay more for a product than it costs to produce? There are multiple answers. The product may be **unique** (there are no other suppliers), it may be the **least costly product of its type available**, consumers may be able to **purchase the product anywhere in the world**, or it may **satisfy some unique needs that other products do not**. Each of these sources of economic value defines a firm's strategy for positioning its products in the marketplace. There are four generic strategies for achieving a profitable business: **differentiation**, **cost**, **scope**, and **focus**. We describe each of these below. The specific strategies that a firm follows will depend on the product, the industry, and the marketplace where competition is encountered.

Although the Internet is a unique marketplace, the same principles of strategy and business apply. As you will see throughout the book, successful e-commerce strategies involve using the Internet and mobile platform to leverage and strengthen existing business (rather than destroy your business), and to provide products and services your competitors cannot copy (in the short term anyway). That means developing unique products, proprietary content, distinguishing processes (such as Amazon's one-click shopping), and personalized or customized services and products (Porter, 2001). There are five generic business strategies: product/service differentiation, cost competition, scope, focus, and customer/supplier intimacy. Let's examine these ideas more closely.

Differentiation refers to all the ways producers can make their products or services unique and distinguish them from those of competitors. The opposite of differentiation is **commoditization**—a situation where there are **no differences among products or services**, and the only basis of choosing is **price**. As economists tell us, when price alone becomes the basis of competition and there are many suppliers and

business strategy

a set of plans for achieving superior long-term returns on the capital invested in a business firm

profit

the difference between the price a firm is able to charge for its products and the cost of producing and distributing goods

Sources of the Economic Value

differentiation

refers to all the ways producers can make their products or services unique and different to distinguish them from those of competitors

commoditization

a situation where there are no differences among products or services, and the only basis of choosing is price

many customers, eventually the price of the good/service falls to the cost to produce it (marginal revenues from the n th unit equal marginal costs). And then profits are zero! This is an unacceptable situation for any business person. The solution is to differentiate your product or service and to create a monopoly-like situation where you are the only supplier.

There are many ways businesses differentiate their products or services. A business may start with a core generic product or service, but then create expectations among users about the “experience” of consuming the product or using the service—“Nothing equals the experience of driving a BMW.” Businesses may also augment products and services by adding features to make them different from those of competitors. And businesses can differentiate their products and services further by enhancing their abilities to solve related consumer problems. For instance, tax programs such as TurboTax can import data from spreadsheet programs, as well as be used to file tax returns online. These capabilities are enhancements to the product that solve a customer’s problems. The purpose of marketing is to create these differentiation features and to make the consumer aware of the unique qualities of products and services, creating in the process a “brand” that stands for these features. We discuss marketing and branding in Chapters 6 and 7.

In their totality, the differentiation features of a product or service constitute the customer value proposition we described in earlier sections of this chapter. E-commerce offers some unique ways to differentiate products and services, such as the ability to personalize the shopping experience and to customize the product or service to the particular demands of each consumer. E-commerce businesses can also differentiate products and services by making it possible to purchase the product from home, work, or on the road (ubiquity); by making it possible to purchase anywhere in the world (global reach); by creating unique interactive content, videos, stories about users, and reviews by users (richness and interactivity); and by storing and processing information for consumers of the product or service, such as warranty information on all products purchased through a site or income tax information online (information density).

Adopting a **strategy of cost competition** means a business has discovered some unique set of business processes or resources that other firms cannot obtain in the marketplace. Business processes are the atomic units of the value chain. For instance, the set of value-creating activities called **Inbound Logistics** in Figure 2.5 is in reality composed of many different collections of activities performed by people on the loading docks and in the warehouses. These different collections of activities are called *business processes*—the set of steps or procedures required to perform the various elements of the value chain.

When a firm discovers a new, more efficient set of business processes, it can obtain a cost advantage over competitors. Then it can attract customers by charging a lower price, while still making a handsome profit. Eventually, its competitors go out of business as the market decisively tilts toward the lowest-cost provider. Or, when a business discovers a unique resource, or lower-cost supplier, it can also compete effectively on cost. For instance, switching production to low-wage-cost areas of the world is one way to lower costs.

What are the ways that E-commerce follows to differentiate the products or services?

strategy of cost competition

offering products and services at a lower cost than competitors

Business processes = resources

Competing on cost can be a short-lived affair and very tricky. Competitors can also discover the same or different efficiencies in production. And competitors can also move production to low-cost areas of the world. Also, competitors may decide to lose money for a period as they compete on cost.

E-commerce offers some ways to compete on cost, at least in the short term. Firms can leverage ubiquity by lowering the costs of order entry (the customer fills out all the forms, so there is no order entry department); leverage global reach and universal standards by having a single order entry system worldwide; and leverage richness, interactivity, and personalization by creating customer profiles online and treating each individual consumer differently—without the use of an expensive sales force that performed these functions in the past. Finally, firms can leverage information intensity by providing consumers with detailed information on products, without maintaining either expensive catalogs or a sales force.

While e-commerce offers powerful capabilities for intensifying cost competition, which makes cost competition appear to be a viable strategy, the danger is that competitors have access to the same technology. The factor markets—where producers buy supplies—are open to all. Assuming they have the skills and organizational will to use the technology, competitors can buy many of the same cost-reducing techniques in the marketplace. Even a skilled labor force can be purchased, ultimately. However, self-knowledge, proprietary tacit knowledge (knowledge that is not published or codified), and a loyal, skilled workforce are in the short term difficult to purchase in factor markets. Therefore, cost competition remains a viable strategy.

Two other generic business strategies are scope and focus. A scope strategy is a strategy to compete in all markets around the globe, rather than merely in local, regional, or national markets. The Internet's global reach, universal standards, and ubiquity can certainly be leveraged to assist businesses in becoming global competitors. Yahoo, for instance, along with all of the other top 20 e-commerce companies, has readily attained a global presence. A focus/market niche strategy is a strategy to compete within a narrow market segment or product segment. This is a specialization strategy with the goal of becoming the premier provider in a narrow market. For instance, L.L.Bean uses e-commerce to continue its historic focus on outdoor sports apparel; and W.W. Grainger focuses on the narrow MRO market segment. E-commerce offers some obvious capabilities that enable a focus strategy. Firms can leverage richness and interactivity to create highly focused messages to different market segments; information intensity makes it possible to focus e-mail and other marketing campaigns on small market segments; personalization—and related customization—means the same product can be customized and personalized to fulfill the very focused needs of specific market segments and consumers.

Another generic strategy is customer intimacy, which focuses on developing strong ties with customers. Strong linkages with customers increase switching costs (the costs of switching from one product or service to a competing product or service) and thereby enhance a firm's competitive advantage. For example, Amazon's one-click shopping that retains customer details and recommendation services based on previous purchases makes it more likely that customers will return to make subsequent purchases.

What are the ways that E-commerce follows to compete on cost?

Even Though most of the competitors have access to the same technology (e.g. factor markets), but still considering cost competitors by competitors is still a viable strategy.. explain?

سر الصنعه

scope strategy

competing in all markets around the globe, rather than just local, regional, or national markets

focus/market niche strategy

competing within a narrow market or product segment

What are the capabilities that E-commerce have to offer a focus strategy?

customer intimacy

focuses on developing strong ties with customers in order to increase switching costs

TABLE 2.9 BUSINESS STRATEGIES		
STRATEGY	DESCRIPTION	EXAMPLE
Differentiation	Making products and services unique and different in order to distinguish them from those of competitors	Warby Parker (vintage-inspired prescription eyeglasses)
Cost competition	Offering products and services at a lower cost than competitors	Walmart
Scope	Competing in all markets around the globe, rather than merely in local, regional, or national markets	Apple iDevices
Focus/market niche	Competing within a narrow market or product segment	Bonobos (men's clothing)
Customer intimacy	Developing strong ties with customers	Amazon; Netflix

Table 2.9 summarizes the five basic business strategies.

Industry structure, industry and firm value chains, value webs, and business strategy are central business concepts used throughout this book to analyze the viability of and prospects for e-commerce companies. In particular, the signature case studies found at the end of each chapter are followed by questions that may ask you to identify the competitive forces in the case, or analyze how the case illustrates changes in industry structure, industry and firm value chains, and business strategy.

E-COMMERCE TECHNOLOGY AND BUSINESS MODEL DISRUPTION

While e-commerce has changed most industries in terms of their structure, processes, and strategies, in some cases e-commerce has radically changed entire industries, driving incumbent firms out of business, greatly altering the economics of an industry, and spawning entirely new firms and value chains (Schumpeter, 1942). When new technologies are at the core of a change in the way business is done, they are referred to as **disruptive technologies**. When the technology involved is digital, the term **digital disruption** is used. Usually it is not the technology per se that is disruptive—in fact, it can be rather ordinary and commonplace. Instead, the disruption occurs when an innovative firm applies the technology to pursue a different business model and strategy than existing firms, perhaps discovering a whole new market that existing firms did not even know existed (Bower and Christensen, 1995; Christensen and Leslie, 2000). For instance, personal computers using off-the-shelf inexpensive processors and technologies disrupted the market for mainframe and mini-computers. All the eight elements of a business model identified previously can be affected by disruptive technologies, from the business value proposition to the revenue model, market opportunity, competitive environment, competitive advantage, market strategy, organizational development, and management. In short, it's a whole new world that often confuses and surprises successful companies who tend to ignore, dismiss, and/or mock

disruptive technologies

technologies that underpin a business model disruption

digital disruption

a business model disruption that is driven by changes in information technology

the early disruptive products. For instance, the entrepreneurs who introduced personal computers identified an entire new market of customers that had been ignored by the large computer firms, along with new price points, competitive factors, and market strategy, using new organizational, management teams, and employees with different skills. Many existing firms could not compete, and dissolved. Similar dynamics can be found in communications (disrupted by e-mail), data storage, music, photography, publishing, and transportation (Lepore, 2014). In 2016, firms like Uber and Airbnb are beginning to have a significant impact on the taxi and lodging industries.

Not all technologies are disruptive (Christensen, et al., 2015; King and Baatartogtokh, 2015). In fact, most successful companies use technology to sustain their current business models, industry structure, processes, and strategies. This use of technology is referred to as **sustaining technology** because it helps companies to cope with competitive pressures and improve their products, and serve their customers with less expensive, more powerful, or unique products. But the same technology can be used by innovative entrepreneurs (**disruptors**) to destroy existing business models. Here's how it works.

Successful companies use whatever technology is available to incrementally improve their products, focusing on the customer by improving quality, price, and service. The incumbent and dominant firms seek to maintain the status quo in an industry, and their firms. In the first disruptive stage, disruptors, often funded by new sources of finance, introduce new products that are less expensive, less capable, and of poorer quality. The first personal computers used relatively unsophisticated technology compared to mainframe computers of the 1970s. These early products nevertheless find a niche in a market that incumbents do not serve or are unaware of. In the second stage, disruptors improve their products at a rapid pace, taking advantage of newer technologies at a faster pace than incumbents, expanding their niche market, and eventually attracting a larger customer base from the incumbents' market. When word processors, and eventually Microsoft Office, were married to the more powerful PC of the 1980s, they attracted a new market of business managers and professionals that was not served by incumbents. The concept was entirely new at the time. The successful incumbents never thought business professionals, let alone people working at home, would like to have a computer at their desk to create documents, build spreadsheets, and make presentation slides. The people and companies that developed personal computers were outsiders to the mainframe computer industry. They were disruptors. They had the vision.

In the third stage, the new products and business model become good enough, and even superior to products offered by incumbents. In the fourth stage, incumbent companies lose market share, and either go out of business or are consolidated into other more successful firms that serve a much more limited customer base. Some incumbents survive by finding new customers for their existing product, adopting some of the newer products and business models in separate divisions of their firms, or moving into other often nearby markets. For instance, mainframe computers are still made by IBM, but they are one of the few survivors. They survived by sustaining innovation in their traditional market of large-scale computing for Fortune 500 firms, moving into computing services, data centers, enterprise software, and most recently cloud computing, business analytics, data mining, and machine learning. As for the PC

sustaining technologies

technologies that enable the incremental improvement of products and services

disruptors

the entrepreneurs and their business firms that lead a business model disruption

industry, it is currently being disrupted by smartphones and tablet computers, created by outsiders who played a small role in the personal computer world, and who have identified huge consumer markets that incumbent PC manufacturers did not realize even existed. They have the vision, for now, but they face new digital disruptors sure to follow.

Why don't the existing companies realize the changes that are coming, and take steps to compete directly with the disruptors? Successful incumbents usually have enormous capital reserves, in-depth technology and intellectual skills, and access to prestigious management consulting firms. Why didn't Kodak see the transition to digital photography? Why didn't Canon see the smartphone camera as a powerful competitor to digital cameras? Why don't firms disrupt their own business models? The answers are complex. Incumbent technologists and professionals may be trained in an *unfit fitness*, having the wrong skills for the current environment. Shareholders expect returns on investment, not destruction of a firm's historic and cherished profitable products. The existing customer base comes to expect continuous improvement in existing products—not a business disruption, but business as usual. These powerful practices, all of which make good business sense, prevent incumbent firms from meeting the challenges of business model disruption. It is unclear at this time if the two most innovative firms in the current e-commerce environment, Apple and Google, will prove any different from previous incumbents.

2.5

CASE STUDY

Freemium

Takes Pandora Public

Pandora is the Internet's most successful radio service. As of June 2016, it had over 250 million registered users (225 million of whom access the service via a mobile device) and about 80 million active listeners. According to a recent survey, Pandora is the clear leader among Internet radio services, with more than 25% of reporting they had listened to it in the previous week, with Spotify a distant second at 10%. Pandora currently accounts for a 10% share of total U.S. radio listening (both traditional and Internet). In 2015, it streamed over 21 billion hours of music!

At Pandora, users select a genre of music based on a favorite musician, and a computer algorithm puts together a personal radio station that plays not only the music of the selected artist but also closely related music by different artists. Listeners have created over 10 billion different stations. A team of approximately 25 professional musicians listens to new songs each day and classifies the music according to more than 450 musical criteria. These criteria are used in a computer algorithm to classify new songs into various genres. Within each of these genres are hundreds of subgenres. Altogether, Pandora has a database of over 1 million analyzed songs from over 200,000 artists.



Pandora's founders, Will Glaser and Tim Westergren, launched Pandora in 2005. Their biggest challenge was making a business out of a totally new kind of online radio station when competing online stations were making music available for free, many without advertising, and online subscription services were streaming music for a monthly fee and finding some advertising support as well. Online music illegally downloaded from P2P networks for free was also a significant factor, as was iTunes, which by 2005 was a roaring success, charging 99 cents a song. The idea of a "personal" radio station playing your kind of music was very new.

Pandora's business strategy is referred to as "freemium." A freemium strategy is based on giving away some products or services for free while relying on a certain percentage of customers to pay for premium versions of the same product or service. Because the marginal cost of digital products is typically close to zero, providing free product does not cost much, and potentially enables you to reach many more people. If the market is very large, even getting just 1% of that market to purchase could be very lucrative. Other notable freemium success stories include LinkedIn, a social network for career-oriented and job networking that offers some basic services for free, such as creating a profile and making connections, but which charges for premium services, and Dropbox, a cloud storage and file sharing service that provides 2 gigabytes of cloud storage for free, but charges for additional storage. Freemium has been the standard business model for most apps, with over 65% of the top 100 apps in Apple's App Store and the most successful mobile gaming apps today using a freemium strategy.

Pandora's first strategy was to give away 10 hours of free access, and then ask subscribers to pay \$36 a month for a year after they used up their free 10 hours. The result: 100,000 people listened to their 10 hours for free and then refused to pay for the annual service. People loved Pandora but appeared unwilling to pay for it.

Facing financial collapse, in November 2005 Pandora introduced an ad-supported option. Subscribers could listen to a maximum of 40 hours of music in a calendar month for free. After the 40 hours were used up, subscribers had three choices: (a) pay 99 cents for the rest of the month, (b) sign up for a premium service offering unlimited usage, or (c) do nothing. If they chose (c), the music would stop, but users could sign up again the next month. The ad-supported business model was a risky move because Pandora had no ad server or accounting system, but it attracted so many users that in a few weeks it had a sufficient number of advertisers (including Apple) to pay for its infrastructure. In 2006, Pandora added a "Buy" button to each song being played and struck deals with Amazon, iTunes, and other online retail sites. Pandora now gets an affiliate fee for directing listeners to Amazon where users can buy the music. In 2008, Pandora added an iPhone app to allow users to sign up from their smartphones and listen all day if they wanted. By 2009, this "free" ad-supported model had attracted 20 million users.

After attracting a sufficiently large user base, Pandora turned its attention back to its premium service. In late 2009, the company launched Pandora One, a high-end version of its service that offered no advertising, higher-quality streaming music, a desktop app, and fewer usage limits. The service cost \$36 a year. This time around it met with much more success, so much so that Pandora went public in June 2011. By 2016, Pandora had a projected \$1.42 billion in revenue with about 80% coming from advertising and the remainder from subscriptions and other sources.

However, Pandora has not yet shown a profit, and its stock price has steadily dropped since its high in 2014. The company is experiencing slowing growth rates and even declines in its number of active users, and competitors like Spotify have made gains at Pandora's expense. Fully paid services like Apple-backed Apple Music, as well as much-hyped new entrants like Tidal, founded by Jay Z and a slew of other high profile artists, represent threats to Pandora as well. But the picture isn't totally bleak: Pandora has continued to show growth in advertising revenue and in listener hours, as its active users are listening more and more. Pandora also made a flurry of acquisitions in 2015, including on-demand music service Rdio. Absorbing Rdio signified Pandora's ambitions to directly compete with Spotify in on-demand music streaming, as opposed to focusing primarily on its radio model. Additionally, music licensing costs were expected to increase sharply in 2016, jeopardizing Pandora's ability to license its music, but a 2015 ruling by the U.S. Copyright Royalty Board raised rates to stream a song one time by a smaller amount than expected. After the ruling, Pandora made deals with the two largest music licensing companies in the United States and continues to make deals with music labels in 2016 as it prepares for the launch of its on-demand service.

While freemium clearly has worked to grow companies like Pandora, LinkedIn, and Dropbox, there is ongoing debate about the effectiveness of the freemium strategy. The crux of the issue is that while freemium can be an efficient way to gather a large group of potential customers, companies have found that it's a challenge to convert eyeballs into those willing to pay. Absent subscriber revenue, firms are forced to rely on advertising revenues.

Apple has led a recent push against freemium competitors. Pandora and Spotify have thrived at the expense of iTunes Music Store, whose revenues have declined steeply for several years, and Apple's first attempt at a streaming service, iTunes Radio, was a bust. Undeterred and sensing a shift in the industry, in 2014 Apple acquired Beats, a streaming music service and maker of popular headphones, for \$3 billion. In 2015, Apple launched its own paid subscription streaming service app modeled after Beats called Apple Music, and by offering free three-month trials, quickly made significant inroads against Pandora and Spotify. In 2016, Apple Music has more than 15 million paying users and continues to grow quickly.

Music industry leadership is also unsure about the future of freemium music streaming. The heads of Universal Music Group and Sony Music both expressed skepticism of the long-term prospects of the freemium model in 2015, and in 2014, Taylor Swift removed her entire catalog of music from Spotify in protest of the freemium model, claiming that it devalued her music. Lesser known artists are equally upset with the revenue sharing models used by Pandora and other online music streaming services, with Pandora keeping about 54% of its revenue and only 4% going to music creators. Music labels are optimistic about Apple's ability to make paid streaming work, given Apple's deep pockets and brand cachet. But industry analysts believe that Pandora and Spotify are headed toward profitability as their subscriber numbers continue to expand.

Whether freemium services continue to breathe life back into the music business remains to be seen, but other companies like MailChimp show how freemium can turn

SOURCES: "Pandora's Share of U.S. Radio Listening Time from 1st Quarter 2013 to 4th Quarter 2015," Statista.com, accessed August 22, 2016; "Form 10-Q for the Quarterly Period Ended June 30, 2016," Pandora Media, Inc., July 26, 2016; "US Usage, Sales and Ad Spending Trends for Digital Music, Digital Radio, and Podcasting," by eMarketer, Inc., May 20, 2016; "Pandora Reports Q4 and Full Year 2015 Financial Results," Businesswire.com, February 11, 2016; "The Battle of Subscription Business Models: A Look at Their Strengths and Weaknesses," by Glenn Peoples, Billboard.com, January 29, 2016;

"203 Billion Emails in a Year: The Untold Growth Story of Mailchimp," *Appviral.com*, December 24, 2015; "2016 Is Shaping Up to Be a Critical Year for Pandora, If Not All Music Streaming," by Amy X. Wang, *Quartz.com*, December 23, 2015; "A Big Music Copyright Ruling Has Managed to Make Both Pandora and Record Labels Happy – Mostly," by Amy X. Wang, *Quartz.com*, December 16, 2015; "Pandora to Acquire Pieces of Rdio," by Ienn Peoples, *Billboard.com*, November 16, 2015; "How Freemium Nearly Caused Our Business to Implode," by Josh Pigford, *Baremetrics.com*, November 10, 2015; "Freemium Model Works for Pandora But Is Devastating to Songwriters," by David Israelite, *Hypebot.com*, September 2015; "Should You Consider a Freemium Model For Your Business?" by Chuck Cohn, *Forbes*, July 2, 2015; Amy X. Wang, "No, Apples Music Streaming App Looks Nothing Like Beats," by Liz Stinson, *Wired.com*, June 11, 2015; "Pandora's Three Biggest Issues Are Both a Blessing and a Curse," by Leon Lazaroff, *Thestreet.com*, May 20, 2015; "Spotify: Freemium Clampdown Rumours Are 'Completely False,'" by Tim Ingham, *Musicbusiness-worldwide.com*, May 17, 2015; "Apple, Spotify, and the Battle Over Freemium," by Jingping Zhang, *Harvard Business Review*, May 13, 2015; "Why Apple Wants to End the Era of Free Music Streaming," by James Cook, *Businessinsider.com*, May 5, 2015; "Apple Pushing Music Labels to Kill Free Spotify Streaming Ahead of Beats Relaunch," by Micah Singleton, *Theverge.com*, May 4, 2015; "Apple and Beats Developing Streaming Music Service to Rival Spotify," by Ben Sisario and Brian X. Chen, *New York Times*, March 25, 2015; "Sony Music Boss Doug Morris: 'In General, Free is Death,'" by Stuart Dredge, *Musically.com*, March 12, 2015; "Making 'Freemium' Work," by Vineet Kumar, *Harvard Business Review*, May 2014; "How MailChimp Learned to Treat Data Like Orange Juice and Rethink the Email in the Process," by Derrick Harris, *Gigaom.com*, May 5, 2013; "When Freemium Fails," by Sarah E.

a company's fortunes around. The company lets anyone send e-mail to customers, manage subscriber lists, and track the performance of an e-mail marketing campaign. Despite the powerful tools it gives marketers, and its open applications programming interface, after 10 years in business, the company had only 85,000 paid subscribers.

In 2009, MailChimp began giving away its basic tools and charging subscription fees for special features, expecting that users would be more willing to pay for analytics and other services as their e-mail lists grew. In just over a year, MailChimp went from 85,000 to 450,000 users. E-mail volume went from 200 million a month to around 700 million. Most importantly, the number of paying customers increased more than 150%, while profit increased more than 650%!

For MailChimp, freemium has been worth the price. It currently supports more than 8 million subscribers worldwide, sending over 200 billion e-mails per year. However, Baremetrics, a developer of analytics compatible with the Stripe payment processing platform, came to a different conclusion. Though it had historically charged even for the lowest tier of its product offerings, Baremetrics introduced a free option in 2015. For the full versions of each of the features in the free plan, customers would have to upgrade. If judged solely by conversion rate, the free plan could have been deemed a success, as over 11% of free plan subscribers eventually became paying customers compared to the 3% to 5% that is typical in the industry. However, Baremetrics wasn't able to keep up with the sudden increase in data processing requirements, and the staff it had available for customer support requests were struggling to meet the higher demand.

Eventually, the total number of Baremetrics customers began to drop below what it had been before the introduction of the free plan as frustrated customers canceled their subscriptions. Baremetrics discovered that its resources were too tight to use the freemium model. Unlike MailChimp or Pandora, whose marginal costs were small enough that they could launch their service for millions of users, Baremetrics is a smaller company with different goals and scope. Baremetrics has since switched to a 14-day free trial strategy, after which customers are forced to pick a paid subscription plan.

So when does it make sense to include freemium in a business plan? It makes sense when the product is easy to use and has a very large potential audience, preferably in the millions. Using a freemium strategy can be a very successful marketing tool, because free features can help attract a user base, and are more attractive to most consumers than 30-day free trials that require a cancellation process. A solid customer value proposition is critical. It's helpful if a large user network increases the perceived value of the product (i.e., a dating service such as Match). Freemium may work when a company has good long-term customer retention rates and the product produces more value over time. An extremely important part of the equation is that the variable costs of providing the product or service to additional customers for free must be low.

Companies also face challenges in terms of determining what products and/or services to offer for free versus what to charge for (this may change over time), the cost of supporting free customers, and how to price premium services. Further, it is difficult to predict attrition rates, which are highly variable at companies using freemium. So, while freemium can be a great way to get early users and to provide a company with

a built-in pool for upgrades, it's tough to determine how many users will be willing to pay and willing to stay.

A freemium strategy makes sense for companies such as Pandora, where there is a very low marginal cost, approaching zero, to support free users. It also makes sense for a company where the value to its potential customers depends on a large network, like LinkedIn. Freemium also works when a business can be supported by the percentage of customers who are willing to pay, like Pandora, especially when there are other revenues like advertising fees that can make up for shortfalls in subscriber revenues. The freemium music streaming services don't have to worry about their business model being sound strategy, but they do have to worry about industry goliaths like Apple and the record labels taking a stand against them.

Needleman and Angus Loten, *Wall Street Journal*, August 22, 2012; "Pandora IPO Prices at \$16; Valuation \$2.6 Billion," by Eric Savitz, *Blogs.forbes.com*, June 14, 2011; "Going Freemium: One Year Later," by Ben Chestnut, *Blog.mailchimp.com*, September 27, 2010; "Case Studies in Freemium: Pandora, Dropbox, Evernote, Automattic and MailChimp," by Liz Gannes, *Gigaom.com*, March 26, 2010; *Free: The Future of a Radical Price*, by Chris Anderson, Hyperion, 2009.

Case Study Questions

1. Compare Pandora's original business model with its current business model. What's the difference between "free" and "freemium" revenue models?
2. What is the customer value proposition that Pandora offers?
3. Why did MailChimp ultimately succeed with a freemium model but Baremetrics did not?
4. What's the most important consideration when considering a freemium revenue model?

2.6 REVIEW

KEY CONCEPTS

■ Identify the key components of e-commerce business models.

A successful business model effectively addresses eight key elements:

- *Value proposition*—how a company's product or service fulfills the needs of customers. Typical e-commerce value propositions include personalization, customization, convenience, and reduction of product search and price delivery costs.
- *Revenue model*—how the company plans to make money from its operations. Major e-commerce revenue models include the advertising model, subscription model, transaction fee model, sales model, and affiliate model.
- *Market opportunity*—the revenue potential within a company's intended marketplace.
- *Competitive environment*—the direct and indirect competitors doing business in the same marketplace, including how many there are and how profitable they are.
- *Competitive advantage*—the factors that differentiate the business from its competition, enabling it to provide a superior product at a lower cost.

- *Market strategy*—the plan a company develops that outlines how it will enter a market and attract customers.
 - *Organizational development*—the process of defining all the functions within a business and the skills necessary to perform each job, as well as the process of recruiting and hiring strong employees.
 - *Management team*—the group of individuals retained to guide the company's growth and expansion.
- Describe the major B2C business models.

There are a number of different business models being used in the B2C e-commerce arena. The major models include the following:

- *Portal*—offers powerful search tools plus an integrated package of content and services; typically utilizes a combined subscription/advertising revenue/transaction fee model; may be general or specialized (vortal).
- *E-tailer*—online version of traditional retailer; includes virtual merchants (online retail store only), bricks-and-clicks e-tailers (online distribution channel for a company that also has physical stores), catalog merchants (online version of direct mail catalog), and manufacturers selling directly to the consumer.
- *Content provider*—information and entertainment companies that provide digital content; typically utilizes an advertising, subscription, or affiliate referral fee revenue model.
- *Transaction broker*—processes online sales transactions; typically utilizes a transaction fee revenue model.
- *Market creator*—uses Internet technology to create markets that bring buyers and sellers together; typically utilizes a transaction fee revenue model.
- *Service provider*—offers services online.
- *Community provider*—provides an online community of like-minded individuals for networking and information sharing; revenue is generated by advertising, referral fees, and subscriptions.

■ Describe the major B2B business models.

The major business models used to date in the B2B arena include:

- *E-distributor*—supplies products directly to individual businesses.
- *E-procurement*—single firms create digital markets for thousands of sellers and buyers.
- *Exchange*—independently owned digital marketplace for direct inputs, usually for a vertical industry group.
- *Industry consortium*—industry-owned vertical digital market.
- *Private industrial network*—industry-owned private industrial network that coordinates supply chains with a limited set of partners.

■ Understand key business concepts and strategies applicable to e-commerce.

E-commerce has had a major impact on the **business environment** in the last decade, and have affected:

- *Industry structure*—the nature of players in an industry and their relative bargaining power by changing the basis of competition among rivals, the barriers to entry, the threat of new substitute products, the strength of suppliers, and the bargaining power of buyers.
- *Industry value chains*—the set of activities performed in an industry by suppliers, manufacturers, transporters, distributors, and retailers that transforms raw inputs into final products and services by reducing the cost of information and other transaction costs.
- *Firm value chains*—the set of activities performed within an individual firm to create final products from raw inputs by increasing operational efficiency.
- *Business strategy*—a set of plans for achieving superior long-term returns on the capital invested in a firm by offering unique ways to differentiate products, obtain cost advantages, compete globally, or compete in a narrow market or product segment.

QUESTIONS

1. What is a business model? How does it differ from a business plan?
2. What are the eight key components of an effective business model?
3. What are Amazon's primary customer value propositions?
4. Describe the five primary revenue models used by e-commerce firms.
5. Why is targeting a market niche generally smarter for a community provider than targeting a large market segment?
6. Would you say that Amazon and eBay are direct or indirect competitors? (You may have to visit the websites or apps to answer.)
7. What are some of the specific ways that a company can obtain a competitive advantage?
8. Besides advertising and product sampling, what are some other market strategies a company might pursue?
9. How do venture capitalists differ from angel investors?
10. Why is it difficult to categorize e-commerce business models?
11. Besides the examples given in the chapter, what are some other examples of vertical and horizontal portals in existence today?
12. What are the major differences between virtual storefronts, such as Bluefly, and bricks-and-clicks operations, such as Walmart? What are the advantages and disadvantages of each?
13. Besides news and articles, what other forms of information or content do content providers offer?
14. What is a reverse auction? What company is an example of this type of business?
15. What are the key success factors for exchanges? How are they different from portals?
16. How have the unique features of e-commerce technology changed industry structure in the travel business?
17. Who are the major players in an industry value chain and how are they impacted by e-commerce technology?
18. What are five generic business strategies for achieving a profitable business?
19. What is the difference between a market opportunity and a market space?
20. What is crowdfunding and how does it help e-commerce companies raise capital?

PROJECTS

1. Select an e-commerce company. Visit its website or mobile app and describe its business model based on the information you find there. Identify its customer value proposition, its revenue model, the market space it operates in, who its main competitors are, any comparative advantages you believe the company possesses, and what its market strategy appears to be. Also try to locate information about the company's management team and organizational structure. (Check for a page labeled "the Company," "About Us," or something similar.)
2. Examine the experience of shopping online versus shopping in a traditional environment. Imagine that you have decided to purchase a digital camera (or any other item of your choosing). First, shop for the camera in a traditional manner. Describe how you would do so (for example, how you would gather the necessary information you would need to choose a particular item, what stores you would visit, how long it would take, prices, etc.). Next, shop for the item on the Web or via a mobile app. Compare and contrast your experiences. What were the advantages and disadvantages of each? Which did you prefer and why?
3. During the early days of e-commerce, first-mover advantage was touted as one way to success. On the other hand, some suggest that being a market follower can yield rewards as well. Which approach has

proven to be more successful—first mover or follower? Choose two e-commerce companies that prove your point, and prepare a brief presentation to explain your analysis and position.

4. Select an e-commerce company that has participated in an incubator program such as Y Combinator, TechStars, DreamIt, Capital Factory, or another of your choosing, and write a short report on its business model and the amount and sources of capital it has raised thus far. Include your views on the company's future prospects for success. Then create an elevator pitch for the company.
5. Select a B2C e-commerce retail industry segment such as pet products, sporting goods, or toys, and analyze its value chain and industry value chain. Prepare a short presentation that identifies the major industry participants in that business and illustrates the move from raw materials to finished product.

REFERENCES

- Arthur, W. Brian. "Increasing Returns and the New World of Business." *Harvard Business Review* (July–August 1996).
- Barney, J. B. "Firm Resources and Sustained Competitive Advantage." *Journal of Management* Vol. 17, No. 1 (1991).
- Bellman, Steven, Gerald L. Lohse, and Eric J. Johnson. "Predictors of Online Buying Behavior." *Communications of the ACM* (December 1999).
- Bower, Joseph L., and Clayton Christensen. "Disruptive Technologies: Catching the Wave." *Harvard Business Review* (January–February, 1995).
- Christensen, Clayton M., Michael E. Raynor, and Rory McDonald. "What Is Disruptive Innovation?" *Harvard Business Review* (December 2015).
- eBay, Inc. "eBay Inc. Reports Second Quarter 2016 Results." (July 20, 2016).
- Johnson, Mark, and Clayton Christensen. "Reinventing Your Business Model." *Harvard Business Review* (December 2008).
- Kambil, Ajit, Ari Ginsberg, and Michael Bloch. "Reinventing Value Propositions." Working Paper, NYU Center for Research on Information Systems (1998).
- Kanter, Elizabeth Ross. "The Ten Deadly Mistakes of Wannabes." *Harvard Business Review* (January 2001).
- Kaplan, Steven, and Mohanbir Sawhney. "E-Hubs: The New B2B Marketplaces." *Harvard Business Review* (May–June 2000).
- Kim, W. Chan, and Renee Mauborgne. "Knowing a Winning Business Idea When You See One." *Harvard Business Review* (September–October 2000).
- King, Andrew A. and Baljir Baatartogtokh. "How Useful Is the Theory of Disruptive Innovation?" *Sloan MIT Management Review* (September 15, 2015).
- Lepore, Jill. "The Disruption Machine: What the Gospel of Innovation Gets Wrong." *New Yorker* (June 23, 2014).
- Magretta, Joan. "Why Business Models Matter." *Harvard Business Review* (May 2002).
- Porter, Michael E. "Strategy and the Internet." *Harvard Business Review* (March 2001).
- Porter, Michael E. *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: Free Press (1985).
- Rigdon, Joan I. "The Second-Mover Advantage." *Red Herring* (September 1, 2000).
- Schumpeter, Joseph A. *Capitalism, Socialism and Democracy*. London: Routledge, 1942.
- Teece, David J. "Profiting from Technological Innovation: Implications for Integration, Collaboration, Licensing and Public Policy." *Research Policy* 15 (1986).

PART

2



- **CHAPTER 3**
E-commerce Infrastructure: The Internet, Web, and Mobile Platform
- **CHAPTER 4**
Building an E-commerce Presence: Websites, Mobile Sites, and Apps
- **CHAPTER 5**
E-commerce Security and Payment Systems

Technology Infrastructure for **E-commerce**



CHAPTER

3

E-commerce Infrastructure: The Internet, Web, and Mobile Platform

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Discuss the origins of, and the key technology concepts behind, the Internet.
- Explain the current structure of the Internet.
- Understand the limitations of today's Internet and the potential capabilities of the Internet of the future.
- Understand how the Web works.
- Describe how Internet and web features and services support e-commerce.
- Understand the impact of mobile applications.

The Apple Watch:

Bringing the Internet of Things to Your Wrist

Apple has a rich history of disrupting the technology landscape, dating back to the Mac computer and its revolutionary graphical user interface in the mid-1980s. More recently, we all know about the impact the iPod, iPhone, and iPad have had on our daily lives and on society in general. In 2015, Apple unveiled its most recent attempt at disruptive, groundbreaking technology in the post-Steve Jobs era: the Apple Watch. While so far the Watch has yet to garner the same results as the other iconic Apple products, it has sold relatively well and still offers strong potential to join that group in the future.



© Iain Masterton /Alamy

The Apple Watch is one of the latest examples of wearable computing, a fast-developing field with potential applications in healthcare, medicine, fitness, the military, gaming, and many other areas, especially those requiring the use of both hands. Defined broadly as any electronic technology incorporated into clothing and wearable accessories, examples of wearable technology include wristbands and watches, smart clothing and footwear, and smart glasses. Until recently, wearable technology has been too bulky or unwieldy to be useful, but the proliferation of smaller, more compact, more powerful devices and the resulting improvements in computing power have made wearable computing possible.

Analysts view wearable computing as an industry primed for explosive growth in the near future. According to market research firm IDC, over 100 million wearable computing devices will be shipped by the end of 2016; that number is projected to grow to over 210 million by 2020. The global market for wearable computing products is expected to grow to over \$170 billion by 2021. However, the market for wearable computing is so new and evolving so quickly that even these projections could quickly become obsolete.

Sensing these trends earlier than most, Apple spent several years building and fine-tuning the Apple Watch before releasing it. Ironically, one of the guiding principles behind the development of the Watch is as a counter to the omnipresence of the smartphone, which Apple itself has driven. One of Apple's goals for the Watch is to act as a filter to much of the information overload of a smartphone, only notifying users when truly critical information requires attention. As a result, the Apple Watch prioritizes speed above depth

of engagement. In its development, features that required longer than 10 seconds to use were scrapped in favor of shorter, more concise interactions.

Apple also placed its typical emphasis on elegance and simplicity of design when developing the Watch, both in its outward appearance and its underlying technology. The Watch is equipped with a scrolling wheel called the Digital Crown, which is faster than the touch screen for navigation. It also functions as a button that returns users to the home screen when pressed. Directly underneath the Digital Crown is the Apple Pay button, which allows Watch wearers to quickly pay for transactions. The prominence of the Apple Pay button on the Watch suggests that Apple wants the Watch to become a popular way to make mobile payments.

The Watch screen is a flexible retina display that uses a feature called Force Touch, which allows the Watch to detect the strength of each touch of the screen, performing different functions based on the force of the touch. On the back of the watch are four sensors, consisting of sapphire lenses and photodiode sensors that can monitor the user's vital signs and movements. Movement is used to control many functions of the Watch; for example, when receiving an incoming text message by lifting your arm to view the notification, lowering your arm again will hide the notification, saving it for later. The Watch comes in three price ranges, Sport, Watch, and Edition. Most Watch wearers will opt for the Sport, the basic \$299 model, while the fashion-conscious (and deep-pocketed) may opt for the Edition, a gold-plated version of the Watch that costs between \$10,000 to \$17,000. There are a wide variety of options for watch faces, straps and strap sizes, and other add-ons.

Perhaps the most unique feature of the Apple Watch with regard to the user experience is the Taptic Engine, a form of haptic technology that applies gentle pressure to the skin to deliver information and alerts to the user. Wearers are alerted to different types of incoming information depending on the number, cadence, and force of the taps. Different taps designate incoming phone calls, upcoming meetings, text messages, and news alerts. When using GPS, different taps can designate different steps on the route. The Apple Watch might someday tap you to let you know that you're leaving the house without a winter coat on a cold day, or that your blood sugar is low and you need to eat.

For the time being, many critics of the device rightly point out that nearly all of what the Watch can do, the iPhone can also do, and often do better. On the other hand, because of its compatibility with apps and the Taptic Engine, the capabilities of the Watch in 2020 may be unrecognizable compared to its capabilities in 2016. For instance, sensors in the Watch may be used to differentiate the Watch from the iPhone and iPad, although the new versions of the iPhone are also being equipped with haptic technology.

Major retailers and other app developers have lined up in droves to create Apple Watch apps, despite the fact that the mobile shopping experience can be quite limited on the Watch, and that advertising is limited to ten seconds or less along with all of its other features. The device launched with 3,500 apps already available, including many from major retailers such as eBay, Amazon, and Target. Some online retailers are experimenting with the ability to bookmark an item on the Watch for future viewing on a phone or desktop. Bricks-and-mortar retailers like JCPenney and Kohl's have also developed

SOURCES: "Deep Dive: The Apple Watch Series 2 Delivers on Last Year's Promise," by Michael deAgonia, Computerworld.com, October 21, 2016; "Booming Wearable Computing Market Could Disrupt Multiple Industries," Bccresearch.com, June 8, 2016; "A Year With the Apple Watch: What Works, What Doesn't, and What Lies Ahead?" by Andrew Cunningham, Arstechnica.com, April 22, 2016; "2016 Apple Watch Will Be Internal 'S' Upgrade, Major

apps, and many of these retailers hope to add features that improve the in-store shopping experience for Watch wearers. Users might be able to use a retailer's Watch app to avoid long lines in stores, find items more efficiently with interactive store maps, and pay for their purchases with Apple Pay.

Although the functionality of the Watch may currently be slightly underwhelming, users appear to be extremely satisfied so far, with 97% of Watch wearers reporting satisfaction with their device. That was better than the first iterations of the iPad and the iPhone. The Apple Watch is also selling as well as the Fitbit, a popular fitness tool. Fitbit is also worn around the wrist, but it's considered a "basic" wearable because it cannot run third-party apps. The Apple Watch may grow to have most or all of Fitbit's functionality along with a host of other capabilities. On the other hand, Fitbits sell for as low as \$100 for older models, and work with all types of smartphones, including Androids. The Apple Watch will have to contend with Fitbit and other niche devices from Samsung, Garmin and Xiaomi that may sacrifice some functionality for a much lower cost. Although Apple has not released recent sales figures for the Watch and instead groups them in a category with a host of other products, estimates show that Apple will lead the wearable computing market with just under half of market share in 2016. Nevertheless, most analysts project that thus far, sales have come in under expectations, and the device hasn't really captured the public's attention the way the iPad and iPhone did.

In the early going, Apple focused on making small tweaks, many of which are cosmetic, rather than making wholesale change to the Watch. However, in September 2016, Apple released the Apple Watch 2, with changes that are both internal and external, including a thinner profile, a larger battery, performance enhancements, the addition of extremely efficient micro-LED panels to replace its previous organic LED (OLED) screen, and GPS capability without the use of a nearby iPhone. As the device continues to mature, the Watch is likely to have the functionality that its users demand. Will it be a fitness and health tool? The new frontier in mobile payments? An indispensable in-store shopping buddy? A must-have complement to the iPhone? Or something completely unforeseen? Apple would prefer it be all of these, and become the next great Apple product; but the Watch has a ways to go, both in sales and functionality, until it reaches that level of success.

Design Changes to Wait Until 2017, Insider Says," by Neil Hughes, *Appleinsider.com*, April 11, 2016; "Apple Watch Isn't a Smash Hit, But It Could Be a Sleeper," by Jefferson Graham, *USA Today*, March 18, 2016; "Smartwatch Growth Predicted, Thanks Largely to Apple Watch," by Matt Hamblen, *Computerworld.com*, September 18, 2015; "The Apple Watch Is Already Crushing the Competition, According to a New Study," by Lisa Eadicicco, *Businessinsider.com*, August 27, 2015; "In Apple Watch Debut, Signs of a Familiar Path to Success," by Farhad Manjoo, *New York Times*, July 22, 2015; "How Ecommerce Marketers Are Adapting to the Apple Watch," by Eric Samson, *Entrepreneur.com*, June 03, 2015; "Are Wearables the Next In-Store Shopping Buddies?" *eMarketer, Inc.*, May 29, 2015; "Are We Really Going to Shop From the Apple Watch? What Retail Apps are Trying to Achieve," by Rachel Arthur, *Forbes*, May 7, 2015; "iPhone Killer: The Secret History of the Apple Watch," David Pierce, *Wired.com*, April 2015; "Apple Watch Is Already Attracting E-Commerce Players," by Rebecca Borison, *Thestreet.com*, April 24, 2015; "Wearables: The Next Mobile Payment Device?" *eMarketer, Inc.*, March 3, 2015; "Taptic, Haptics, and the Body Fantastic: The Real Apple Watch Revolution," by Brian S. Hall, *Macworld.com*, October 3, 2014; "Inside the Apple Watch: The Tech Behind Apple's New Wearable," by Adario Strange, *Mashable.com*, September 9, 2014.

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.

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

Internet

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

TABLE 3.1 TRENDS IN E-COMMERCE INFRASTRUCTURE 2016–2017

BUSINESS
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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.

web hosts

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

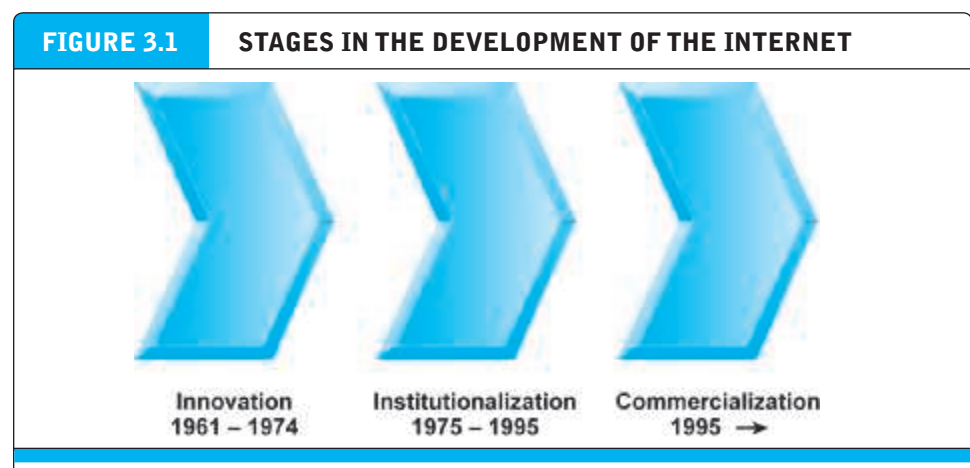
THE EVOLUTION OF THE INTERNET: 1961—THE PRESENT

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.



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
<i>INNOVATION PHASE 1961–1974</i>		
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.
<i>INSTITUTIONALIZATION PHASE 1975–1995</i>		
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.
<i>COMMERCIALIZATION PHASE 1995–PRESENT</i>		
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, anywhere.
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.

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

1

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

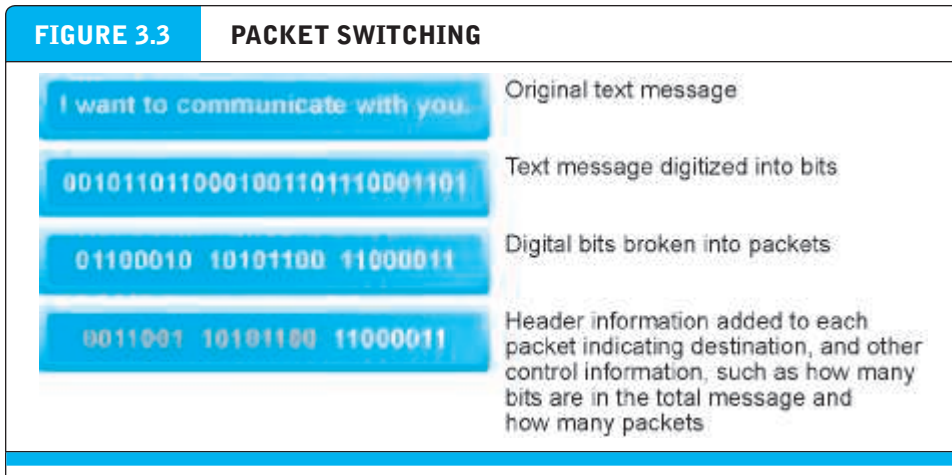
RESOLUTION OF THE FEDERAL NETWORKING COUNCIL

"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.



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.

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

Error control information :
it is done through three techniques:

- 1- Check sum
- 2- Acknowledgment
- 3- Retransmission

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

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.

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

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.

Transmission Control Protocol/Internet Protocol (TCP/IP)

2

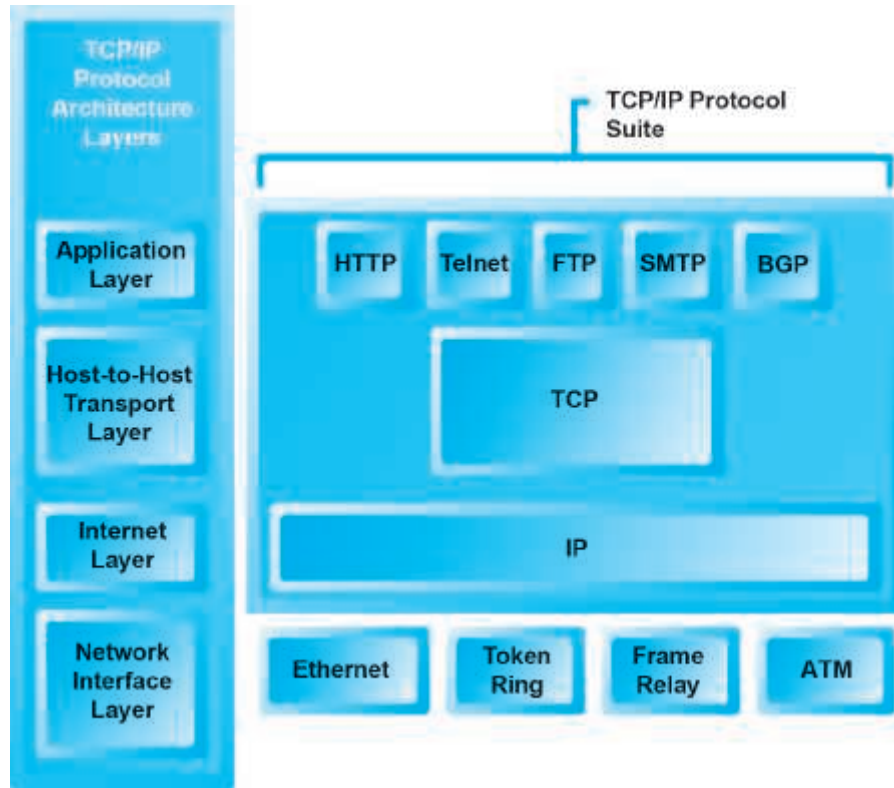
While packet switching was an enormous advance in communications capacity, there was no universally agreed-upon method for breaking up digital messages into packets, routing them to the proper address, and then reassembling them into a coherent message. This was like having a system for producing stamps 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.

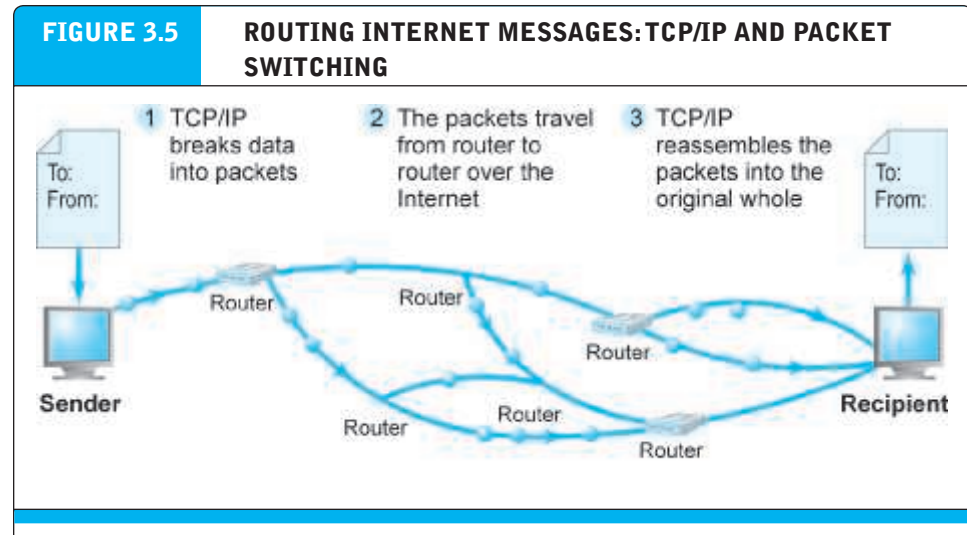
Internet Service Provider. Most corporate and university computers attached to a local area network have a permanent IP address.

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.

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

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



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)

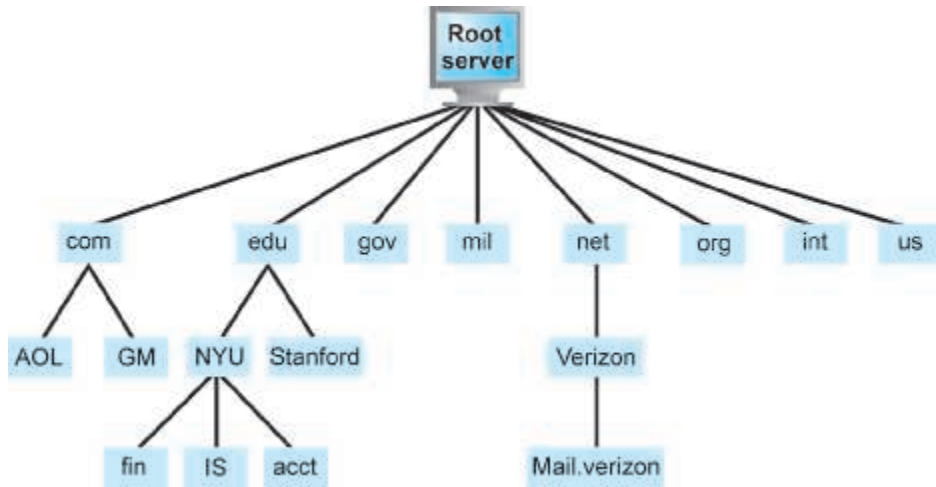
the address used by a web browser to identify the location of content on the Web

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

3

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 <u>unique</u> address number called an Internet Protocol (IP) address.
Domain names	The Domain Name System allows expressions such as <u>Pearsoned.com</u> (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 <u>.com root server</u> . 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

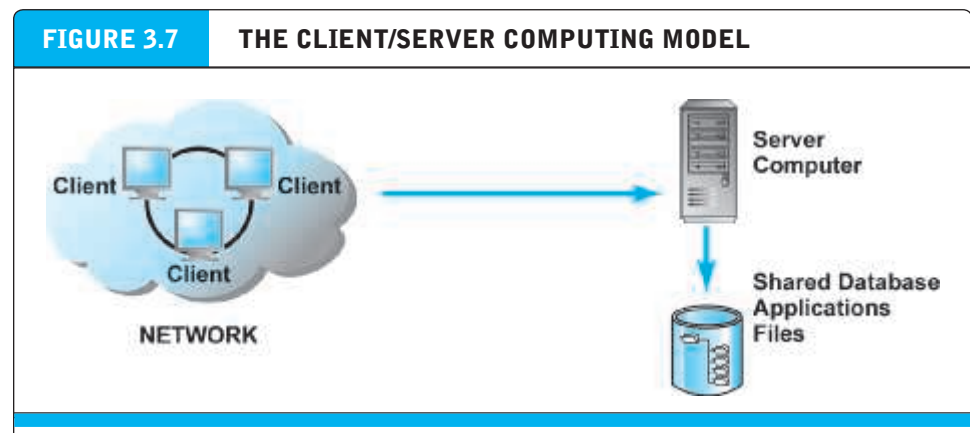
networked computer dedicated to common functions that the client computers on the network need

The advantages for client/server network

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 hyper-linked 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).

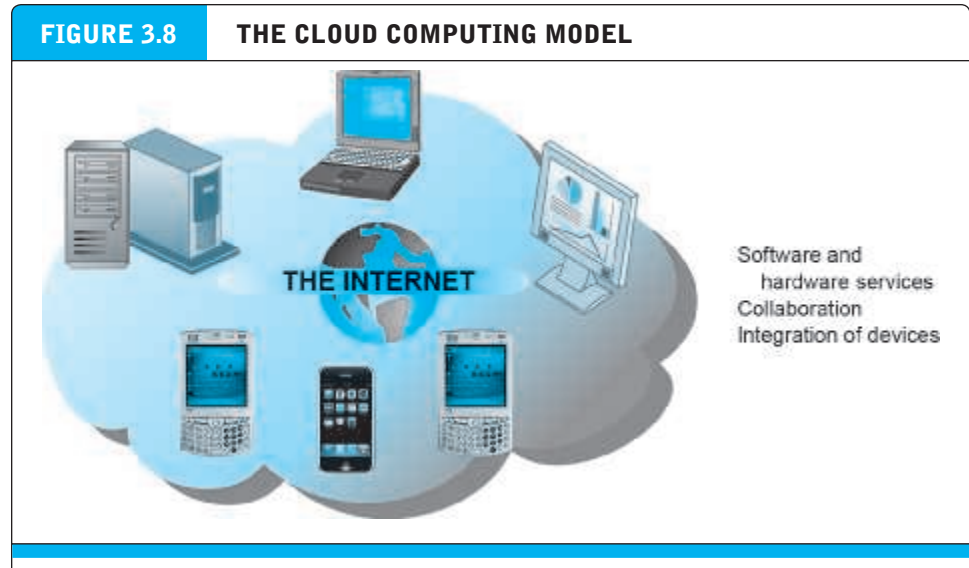
The mobile platform has profound implications for e-commerce because it influences how, where, and when consumers shop and buy.

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



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:

what are the main characteristics of cloud computing?

1 you use it when you need it

2 uses Internet as a medium

3 Resources are pooled together and used by multiple clients

4 Allows elasticity of resources

- **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.

Flexibility

5

Cloud computing consists of three basic types of services:

Delivery Models of cloud computing / Service model

1

- **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

It offers the computing architecture and infrastructure that is it offers all computing resources but in virtual environment so that multiple users can access them.

TABLE 3.4		AMAZON WEB SERVICES
NAME	DESCRIPTION	
<i>COMPUTING SERVICES</i>		
Elastic Compute Cloud (EC2)	Scalable cloud computing services	
Elastic Load Balancing (ELB)	Distributes incoming application traffic among multiple EC2 instances	
<i>STORAGE SERVICES</i>		
Simple Storage Service (S3)	Data storage infrastructure	
Glacier	Low-cost archival and backup storage	
<i>DATABASE SERVICES</i>		
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	
<i>NETWORKING AND CONTENT DELIVERY SERVICES</i>		
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	
<i>ANALYTICS</i>		
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	
<i>APPLICATION SERVICES</i>		
AppStream	Provides streaming services for applications and games from the cloud	
CloudSearch	Search service that can be integrated by developers into applications	
<i>MESSAGING SERVICES</i>		
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.)	
<i>DEPLOYMENT AND MANAGEMENT SERVICES</i>	
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
<i>MOBILE</i>	
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
<i>PAYMENT SERVICES</i>	
Flexible Payment Service (FPS)	Payment services for developers
DevPay	Online billing and account management service for developers who create an Amazon cloud application
<i>MISCELLANEOUS</i>	
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.

on demand service: pay per use of application software to users. **Independent platform:** do not need to install the software on your pc.

- 2 • **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.](#) **so it is cheap**

Google Docs

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

- 3 • **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.

Delivery Models of cloud computing / Deployment model

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

CSP : Content-Security -Policy is the name of HTTP response header that modern browsers use to enhance the security of the document or web page

CSP: Cloud Service Providers

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.

only

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.

private cloud

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

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.

hybrid cloud

offers customers both a public cloud and a private cloud

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 strict Companies that must have control over data sovereignty high authority
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.

Drawbacks of Cloud computing:

2

3

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.

1

The significant implications of cloud computing on e-commerce?

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.

1

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.

1

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)

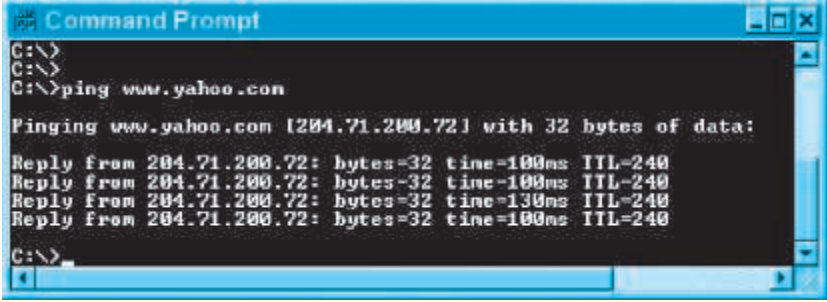
one of the original Internet services. Part of the TCP/IP protocol that permits users to transfer files from the server to their client computer, and vice versa

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


```

Command Prompt
C:\>
C:\>
C:\>ping www.yahoo.com

Pinging www.yahoo.com [204.71.200.72] with 32 bytes of data:
Reply from 204.71.200.72: bytes=32 time=100ms TTL=240
Reply from 204.71.200.72: bytes=32 time=100ms TTL=240
Reply from 204.71.200.72: bytes=32 time=130ms TTL=240
C:\>

```

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.

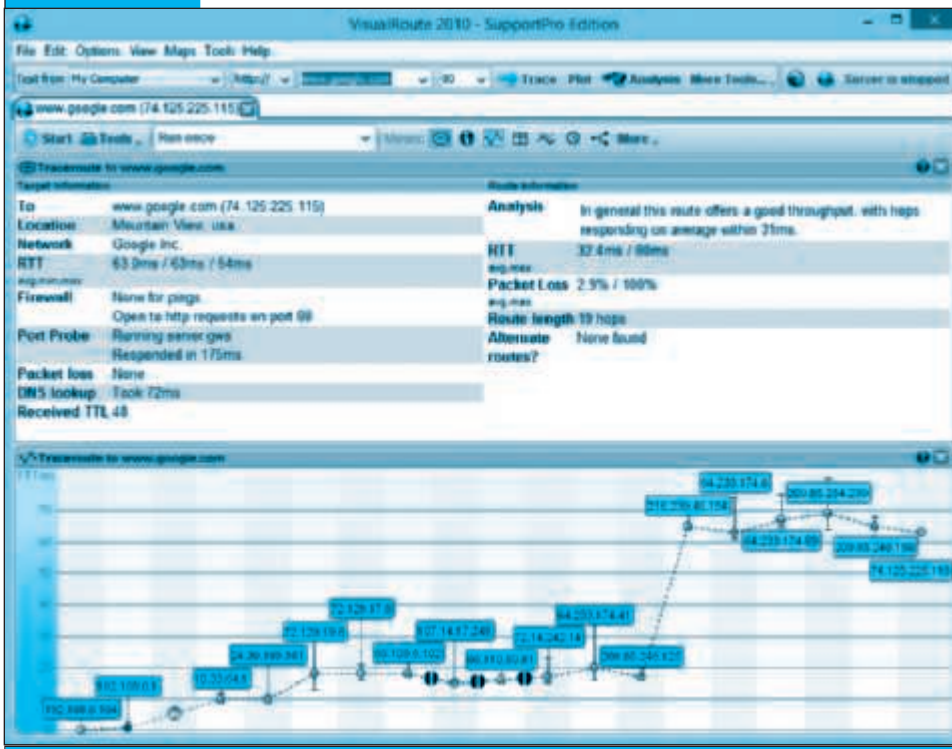
Tracert

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 3.10 TRACING THE ROUTE A MESSAGE TAKES ON THE INTERNET

VisualRoute and other tracing programs provide some insight into how the Internet uses packet switching. This particular message traveled to a Google server in Mountain View, California.

SOURCE: © Visualware, Inc., 2014.

Figure 3.11 illustrates the “hourglass” and layered architecture of the Internet. The Internet can be viewed conceptually as having four layers: Network Technology Substrates, Transport Services and Representation Standards, Middleware Services, and Applications.⁴ The **Network Technology Substrate layer** is composed of telecommunications networks and protocols. The **Transport Services and Representation Standards layer** houses the TCP/IP protocol. The **Applications layer** contains client applications such as the Web, e-mail, and audio or video playback. The **Middleware Services layer** is the glue that ties the applications to the communications networks and includes such services as security, authentication, addresses, and storage repositories. Users work with applications (such as e-mail) and rarely become aware of middleware that operates in the background. Because all layers use TCP/IP and other common standards linking all four layers, it is possible for there to be significant

Network Technology Substrate layer

layer of Internet technology that is composed of telecommunications networks and protocols

Transport Services and Representation Standards layer

layer of Internet architecture that houses the TCP/IP protocol

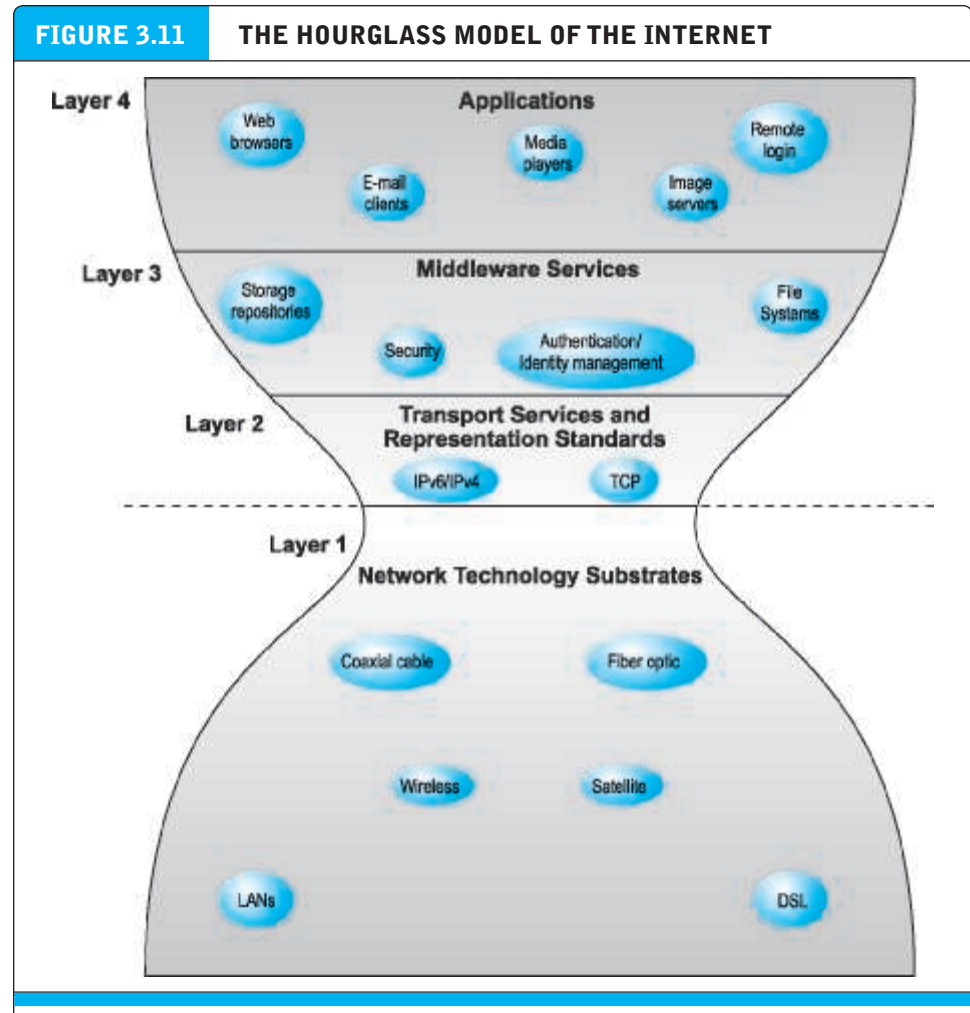
Applications layer

layer of Internet architecture that contains client applications

Middleware Services layer

the “glue” that ties the applications to the communications networks and includes such services as security, authentication, addresses, and storage repositories

⁴ Recall that the TCP/IP communications protocol also has layers, not to be confused with the Internet architecture layers.



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.

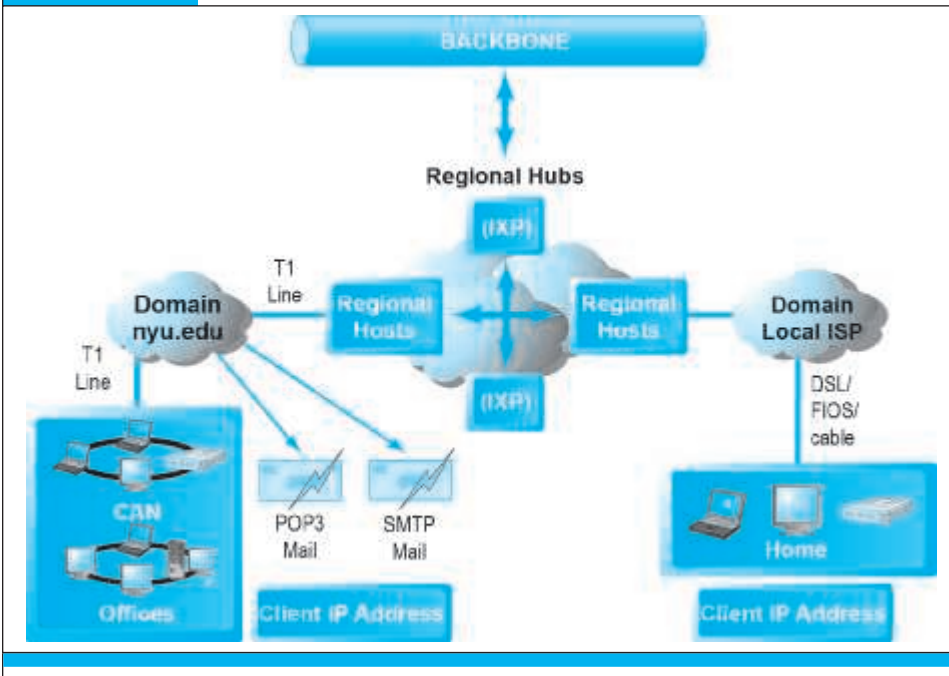
THE INTERNET BACKBONE

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"

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 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	

redundancy

multiple duplicate devices and paths in a network

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).

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 1 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

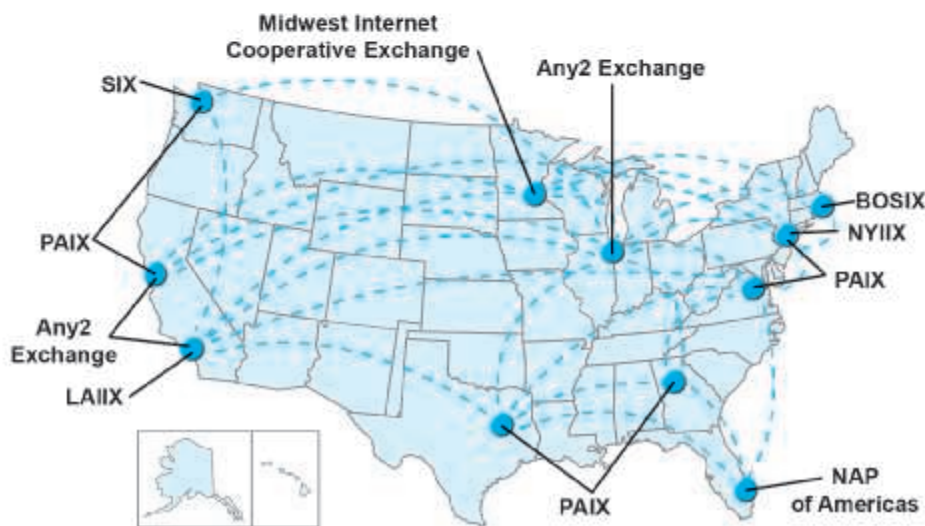


TABLE 3.7 INTERNET ACCESS SERVICE LEVELS AND BANDWIDTH CHOICES		
SERVICE	COST/MONTH	DOWNLOAD SPEED
Telephone modem	\$10–\$25	30–56 Kbps
DSL	\$20–\$30	1–15 Mbps
FiOS	\$50–\$300	25 Mbps–500 Mbps
Cable Internet	\$35–\$199	1 Mbps–500 Mbps
Satellite	\$39–\$129	5–15 Mbps
T1	\$200–\$300	1.54 Mbps
T3	\$2,500–\$10,000	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).

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

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

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.

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.

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.

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.

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.

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

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

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

high-speed broadband Internet access provided via satellite

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

TABLE 3.8 TIME TO DOWNLOAD A 10-MEGABYTE FILE BY TYPE OF INTERNET SERVICE	
TYPE OF INTERNET SERVICE	TIME TO DOWNLOAD
<i>NARROWBAND SERVICES</i>	
Telephone modem	25 minutes
<i>BROADBAND SERVICES</i>	
DSL @ 1 Mbps	1.33 minutes
Cable Internet @ 10 Mbps	8 seconds
T1	52 seconds
T3	2 seconds

These organizations are sufficiently large that they lease access to the Web directly from regional and national carriers. These local area networks generally are running Ethernet (a local area network protocol) and have network operating systems such as Windows Server or Linux that permit desktop clients to connect to the Internet through a local Internet server attached to their campus networks. Connection speeds in campus area networks are in the range of 10–100 Mbps to the desktop.

INTRANETS

The very same Internet technologies that make it possible to operate a worldwide public network can also be used by private and government organizations as internal networks. An **intranet** is a TCP/IP network located within a single organization for purposes of communications and information processing. Internet technologies are generally far less expensive than proprietary networks, and there is a global source of new applications that can run on intranets. In fact, all the applications available on the public Internet can be used in private intranets. The largest provider of local area network software is Microsoft, followed by open source Linux, both of which use TCP/IP networking protocols.

intranet

a TCP/IP network located within a single organization for purposes of communications and information processing

WHO GOVERNS THE INTERNET?

Aficionados and journalists often claim that the Internet is governed by no one, and indeed cannot be governed, and that it is inherently above and beyond the law. What these people forget is that the Internet runs over private and public telecommunications facilities that are themselves governed by laws, and subject to the same pressures as all telecommunications carriers. In fact, the Internet is tied into a complex web of governing bodies, national governments, and international professional societies. There is no one single governing organization that controls activity on the Internet.

Instead, there are a number of organizations that influence the system and monitor its operations. Among the governing bodies of the Internet are:

- The *Internet Corporation for Assigned Names and Numbers (ICANN)*, which coordinates the Internet's systems of unique identifiers: IP addresses, protocol parameter registries, and the top-level domain systems. ICANN was created in 1998 as a non-profit organization and manages the *Internet Assigned Numbers Authority (IANA)*, which is in charge of assigning IP addresses.
- The *Internet Engineering Task Force (IETF)*, which is an open international community of network operators, vendors, and researchers concerned with the evolution of the Internet architecture and operation of the Internet. The IETF has a number of working groups, organized into several different areas, that develop and promote Internet standards, which influence the way people use and manage the Internet.
- The *Internet Research Task Force (IRTF)*, which focuses on the evolution of the Internet. The IRTF has a number of long-term research groups working on various topics such as Internet protocols, applications, applications, and technology.
- The *Internet Engineering Steering Group (IESG)*, which is responsible for technical management of IETF activities and the Internet standards process.
- The *Internet Architecture Board (IAB)*, which helps define the overall architecture of the Internet and oversees the IETF and IRTF.
- The *Internet Society (ISOC)*, which is a consortium of corporations, government agencies, and nonprofit organizations that monitors Internet policies and practices.
- The *Internet Governance Forum (IGF)*, which is a multi-stakeholder open forum for debate on issues related to Internet governance.
- The *World Wide Web Consortium (W3C)*, which is a largely academic group that sets HTML and other programming standards for the Web.
- The *Internet Network Operators Groups (NOGs)*, which are informal groups that are made up of ISPs, IXPs, and others that discuss and attempt to influence matters related to Internet operations and regulation.

While none of these organizations has actual control over the Internet and how it functions, they can and do influence government agencies, major network owners, ISPs, corporations, and software developers with the goal of keeping the Internet operating as efficiently as possible. ICANN comes closest to being a manager of the Internet and reflects the powerful role that the U.S. Department of Commerce has played historically in Internet governance. The United States has been responsible for the IANA function since the beginning of the Internet. After the creation of ICANN, however, the expectation was the function would eventually be transferred out of the U.S. government's control. In 2006, however, the U.S. Department of Commerce announced that the U.S. government would retain oversight over the root servers, contrary to initial expectations. There were several reasons for this move, including the use of the Internet for basic communications services by terrorist groups and the uncertainty that might be caused should an international body take over. In 2008, the Department of Commerce reaffirmed this stance, stating that it did not have

any plans to transition management of the authoritative root zone file to ICANN (U.S. Department of Commerce, 2008). At the same time, growing Internet powers China and Russia were lobbying for more functions of the Internet to be brought under the control of the United Nations, raising fears that governance of the Internet could become even more politicized (Pfanner, 2012). In 2014, the United States, under continued pressure from other countries, finally announced its willingness to transition control of IANA, provided that certain stipulations are met, including that the organization managing the IANA functions not be specifically controlled by any other government or inter-governmental organization (such as the United Nations). The transition took place on October 1, 2016.

In addition to these professional bodies, the Internet must also conform to the laws of the sovereign nation-states in which it operates, as well as the technical infrastructures that exist within each nation-state. Although in the early years of the Internet there was very little legislative or executive interference, this situation is changing as the Internet plays a growing role in the distribution of information and knowledge, including content that some find objectionable.

Read *Insight on Society: Government Regulation and Surveillance of the Internet* for a further look at the issue of censorship of Internet content and substance.

3.3 THE FUTURE INTERNET INFRASTRUCTURE

The Internet is changing as new technologies appear and new applications are developed. The next era of the Internet is being built today by private corporations, universities, and government agencies. To appreciate the potential benefits of the Internet of the future, you must first understand the limitations of the Internet's current infrastructure.

LIMITATIONS OF THE CURRENT INTERNET

Much of the Internet's current infrastructure is several decades old (equivalent to a century in Internet time). It suffers from a number of limitations, including:

- *Bandwidth limitations.* There is insufficient capacity throughout the backbone, the metropolitan switching centers, and most importantly, the “last mile” to the house and small businesses. The result is slow peak-hour service (congestion) and a limited ability to handle high volumes of video and voice traffic.
- *Quality of service limitations.* Today's information packets take a circuitous route to get to their final destinations. This creates the phenomenon of **latency**—delays in messages caused by the uneven flow of information packets through the network. In the case of e-mail, latency is not noticeable. However, with streaming video and synchronous communication, such as a telephone call, latency is noticeable to the user and perceived as “jerkiness” in movies or delays in voice communication. Today's Internet uses “best-effort” quality of service (QoS), which makes no guarantees about when or whether data will be delivered, and provides each packet with the same level of service, no matter who the user is or what type of data is

latency

delays in messages caused by the uneven flow of information packets through the network

INSIGHT ON SOCIETY

GOVERNMENT REGULATION AND SURVEILLANCE OF THE INTERNET

Hardly a week goes by without reports that a massive protest has occurred in the streets of a big city somewhere in the world. Invariably, the Internet, social media, and mobile phones are either blamed or praised for enabling these popular expressions of discontent with political regimes, corrupt officials, unemployment, or wealth inequality. Such events encourage us to think of the Internet and the Web as an extraordinary technology unleashing torrents of human creativity, innovation, expression, popular rebellion, and sometimes, even democracy.

How ironic then that the same Internet has also spawned an explosion in government control and surveillance of individuals on the Internet. Totalitarian dictators of the mid-twentieth century would have given their eyeteeth for a technology such as this, that can track what millions of people do, say, think, and search for in billions of e-mails, searches, blogs, and Facebook posts every day.

In the early years of the Internet and the Web, many people assumed that because the Internet is so widely dispersed, it must be difficult to control or monitor. But the reality is quite different. We now know that just about all governments assert some kind of control and surveillance over Internet content and messages, and in many nations this control over the Internet and the people who use it is very extensive.

While the Internet is a decentralized network, Internet traffic in all countries runs through large fiber-optic trunk lines that are controlled by national authorities or private firms. In China, there are three such lines, and China requires the companies that own these lines to configure their routers for both internal and external service

requests. When a request originates in China for a web page in Chicago, Chinese routers examine the request to see if the site is on a blacklist, and then examine words in the requested web page to see if it contains blacklisted terms. The system is often referred to as "The Great Firewall of China" (but formally by China as the "Golden Shield") and was implemented with the assistance of Cisco Systems (the U.S. firm that is the largest manufacturer of routers in the world), Juniper Networks, and California-based Blue Coat (now owned by Symantec), which provides deep packet inspection software. A number of other U.S. Internet firms have also been involved in China's censorship and surveillance efforts.

Over the past several years, China has strengthened and extended its regulation of the Internet in the name of social stability. Recently passed legislation allows web users to be jailed for up to three years if they post defamatory rumors that are read by more than 5,000 people. China has also issued rules to restrict the dissemination of political news and opinions on instant messaging applications such as WeChat, a text messaging app similar to Twitter and WhatsApp. Users are required to post political opinions and news only to state-authorized media outlets and are required to use their own names when establishing accounts. In 2016, China issued new rules barring foreign companies or their affiliates from publishing online content without government approval. It also began to subject online programs to the same censorship regulations as regular TV shows. In July 2016, it said it would punish websites that publish unverified social media content as news, and ordered several of the most popular Chinese portals, such as Sinu, Sohu, and NetEase, to cease original news reporting.

(continued)



While China is often criticized for its extensive Internet controls, other countries are not far behind. Iran's Internet surveillance of its citizens is considered by security experts to be one of the world's most sophisticated mechanisms for controlling and censoring the Internet, allowing it to examine the content of individual online communications on a massive scale. The Iranian system goes beyond merely preventing access to specific sites such as Google, Twitter, and Facebook and reportedly also utilizes deep packet inspection. Deep packet inspection allows governments to read messages, alter their contents for disinformation purposes, and identify senders and recipients. It is accomplished by installing computers in the line between users and ISPs, opening up every digitized packet, inspecting for keywords and images, reconstructing the message, and sending it on. This is done for all Internet traffic including Skype, Facebook, e-mail, tweets, and messages sent to proxy servers. In 2016, Iran announced that it had completed the first stage of establishing an isolated, domestic version of the Internet, purportedly one that will be faster and less costly, but which subjects its users to even more heightened surveillance.

In Russia, a 2014 law allows the government to close websites without a court decision if the General Prosecutor's office declares the material on a site to be "extremist." Russia also regulates the blogosphere, requiring bloggers with more than 3,000 daily readers to register their real names and contact information with Russia's communications regulator. In 2015, Russia passed laws requiring domestic Internet companies to store their data on Russian soil, allowing the government to control it and limit access, and in July 2016, passed additional laws that provide for mandatory data retention by ISPs and telecommunications providers for between 6 months and three years, require those companies to provide access to all such data without a warrant, and also require a government backdoor that will enable it to access all encrypted communications.

Turkey is another country that has increasingly attempted to control and censor Internet content. These efforts have increased after the terrorist attack on Istanbul's Ataturk Airport and the failed coup against President Recep Tayyip Erdogan.

But it is not just totalitarian nations that have sought to regulate and surveil the Internet. Both Europe and the United States have, at various times, also taken steps to control access to certain websites, censor web content, and engage in extensive surveillance of communications. For instance, Great Britain has a list of blocked sites, as do Germany, France, and Australia. The United States and European countries generally ban the sale, distribution, and/or possession of online child pornography. France, Germany, and Austria all bar the online sale of Nazi memorabilia. Even in South Korea, one of the world's most wired countries, there are restrictions on content that is deemed subversive and harmful to the public order.

In response to terrorism threats and other crimes, European governments and the U.S. government also perform deep packet inspection on e-mail and text communications of terrorist suspects. This surveillance is not limited to cross-border international data flows and includes large-scale domestic surveillance and analysis of routine e-mail, tweets, and other messages. In 2013, National Security Agency (NSA) contractor Edward Snowden made headlines by leaking classified NSA documents shedding light on the NSA's PRISM program, which allowed the agency access to the servers of major Internet companies such as Facebook, Google, Apple, Microsoft, and many others. Additionally, the documents revealed the existence of the NSA's XKeyscore program, which allows analysts to search databases of e-mails, chats, and browsing histories of individual citizens without any authorization. Warrants, court clearance, or other forms of legal documentation are not required for analysts to use the technology. Snowden's documents

also showed spy agencies were tapping data from smartphone apps like Candy Crush, and most others, and that the NSA was tapping the flow of personal user information between Google and Yahoo. The NSA claimed that the program was only used to monitor foreign intelligence targets and that the information it collects has assisted in apprehending terrorists. The FBI also has an Internet surveillance unit, the National Domestic Communications Assistance Center. The NDCAC's mission is to assist in the development of new surveillance technologies that will allow authorities to increase the interception of Internet, wireless, and VoIP communications.

In 2016, many European powers moved ahead with plans to fortify their online surveillance with new start-of-the-art networks. In England, potential new laws would force Internet service companies to maintain "Internet connection records" that would be subject to review by law enforcement at any time. In response to multiple terror attacks on French soils in 2015, the French government passed very similar rules that force ISPs to maintain browsing data, as well as additional provisions for surveillance of phone calls, e-mails, and all mobile phone communications. And De-Cix, the world's largest IXP, pushed back against the German government regarding requests to allow surveillance

of all communications passing through its Frankfurt hub. De-Cix sued the German intelligence service for what it views as illegal overreach, but the German government hopes to pass new laws that would legitimize the practice, just as England, France, and other nations have done.

However, in the United States, efforts are underway to curb domestic and international counter-terrorist agencies like the NSA from conducting dragnet surveillance of the entire American population, strengthen court oversight of surveillance, limit surveillance to specific individuals, and ease disclosure rules for Internet firms who receive requests from government agencies. In 2015, Congress passed the USA Freedom Act, which limits the bulk collection of Americans' phone records. However, equally concerted efforts are underway to expand these types of spying powers. For instance, the Obama administration has expanded the NSA's ability to perform warrantless wiretaps on suspected malicious hackers, allowing them to monitor international Internet traffic from these suspects as well as domestic traffic. Concerns about the use of the Internet and other methods of encrypted communications by the Islamic State to recruit new members and engage in terrorism have further heightened the tension.

SOURCES: "World's Biggest Internet Hub Sues German Government Over Surveillance," by David Meyer, *Fortune*, September 16, 2016; "Iran Launches New 'National Internet' That Censors Content, Encourages Regime Surveillance," *Thetower.org*, August 30, 2016; "China Clamps Down on Online News Reporting," by Michael Forsythe, *New York Times*, July 25, 2016; "Russia Asks for the Impossible with Its New Surveillance Laws," by Eva Galperin and Danny O'Brien, *Eff.org*, July 19, 2016; "China Cracks Down on News Reports Spread via Social Media," by Edward Wong and Vanessa Pia, July 5, 2016; "Britain to Pay Billions for Monster Internet Surveillance Network," by Duncan Campbell, *Computerweekly.com*, March 21, 2016; "China Cracks Down on Online Television," by Amy Qin, *New York Times*, March 3, 2016; "New Chinese Rules on Foreign Firms' Online Content," by David Barboza and Paul Mozer, *New York Times*, February 19, 2016; "ISIS Influence on Web Prompts Second Thoughts on First Amendment," by Erik Eckholm, *New York Times*, December 7, 2015; "France Has a Powerful and Controversial New Surveillance Law," by Arik Hesseldahl, *Recode.net*, November 14, 2015; "Freedom on the Net 2015," *Freedomhouse.org*, October 28, 2015; "Russian Data Law Fuels Web Surveillance Fears," by Shaun Walker, *The Guardian*, September 1, 2015; "China Passes New National Security Law Extending Control Over Internet," *The Guardian*, July 1, 2015; "Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border," by Charlie Savage et al., *New York Times*, June 4, 2015; "The State of Surveillance in Iran," by Arta Shams, *Ifex.org*, May 22, 2015; "House Moves to Curb Government Surveillance of Phone, Internet Records," by Cristina Maza, *Csmonitor.com*, May 1, 2015; "Turkey's Parliament Issues Contested Security, Surveillance Laws," *Bloombergnews.com*, March 27, 2015; "Russia Forces Its Popular Bloggers to Register—Or Else," by Ilya Khrennikov, *Bloomberg.com*, August 19, 2014; "NSA Top Lawyer Says Tech Giants Knew About Data Collection," *Cnet.com*, March 19, 2014; "Documents Say NSA Pretends to Be Facebook in Surveillance," by Reed Albergotti, *Wall Street Journal*, March 12, 2014; "Amid Flow of Leaks, Turkey Moves to Crimp Internet," by Tim Arango and Ceylan Yeginsu, *New York Times*, February 6, 2014; "Spy Agencies Tap Data Streaming From Phone Apps," by James Glanz, Jeff Larson, and Andrew Lehren, *New York Times*, January 27, 2014; "NSA Surveillance Covers 75 Percent of U.S. Internet Traffic: WSJ," by Reuters, *News.Yahoo.com*, August 20, 2013; "New Snowden Leak: NSA Program Taps All You Do Online," by Amanda Wills, *Mashable.com*, August 1, 2013; "Snowden: NSA Collects 'Everything,' Including Content of Emails," by Eyder Peralta, *NPR.org*, June 17, 2013; "FBI Quietly Forms Secret Net-Surveillance Unit," by Declan McCullagh, *News.cnet.com*, May 22, 2012.

contained in the packet. A higher level of service quality is required if the Internet is to keep expanding into new services, such as video on demand and telephony.

- *Network architecture limitations.* Today, a thousand requests for a single music track from a central server will result in a thousand efforts by the server to download the music to each requesting client. This slows down network performance, as the same music track is sent out a thousand times to clients that might be located in the same metropolitan area. This is very different from television, where the program is broadcast once to millions of homes.
- *Wired Internet.* The Internet is still largely based on cables—fiber-optic and coaxial copper cables. Copper cables use a centuries-old technology, and fiber-optic cable is expensive to place underground. The wired nature of the Internet restricts mobility of users although it is changing rapidly as Wi-Fi hotspots proliferate, and cellular phone technology advances. However, cellular systems are often overloaded due to the growth in the number of smartphones.

Now imagine an Internet at least 1,000 times as powerful as today's Internet, one that is not subjected to the limitations of bandwidth, protocols, architecture, physical connections, and language detailed previously. Welcome to the world of the future Internet, and the next generation of e-commerce services and products!

THE INTERNET2® PROJECT

Internet2®

advanced networking consortium of more than 450 member institutions working in partnership to facilitate the development, deployment, and use of revolutionary Internet technologies

Internet2® is an advanced networking consortium of more than 450 member institutions including universities, corporations, government research agencies, and not-for-profit networking organizations, all working in partnership to facilitate the development, deployment, and use of revolutionary Internet technologies. The broader Internet2 community includes more than 90,000 institutions across the United States and international networking partners in more than 100 countries. Internet2's work is a continuation of the kind of cooperation among government, private, and educational organizations that created the original Internet.

The advanced networks created and in use by Internet2 members provide an environment in which new technologies can be tested and enhanced. For instance, Internet2 provides a next-generation, nationwide 100 gigabit-per-second network that not only makes available a reliable production services platform for current high-performance needs but also creates a powerful experimental platform for the development of new network capabilities. See **Table 3.9** to get some sense of just how fast a 100-Gbps network is in terms of data transmission times. The fourth generation of this network, built through a federal stimulus grant from the National Telecommunications and Information Administration's Broadband Technology Opportunities Program, has now been deployed. The hybrid optical and packet network provides 8.8 terabits of capacity with the ability to seamlessly scale as requirements grow, includes over 15,000 miles of owned fiber optic cable, and reaches into underserved areas of the country, supporting connectivity for approximately 200,000 U.S. community anchor institutions (schools, local libraries, and museums), and enabling them to provide citizens across the country with telemedicine, distance learning, and other advanced applications not possible with consumer-grade Internet services. The infrastructure supports a wide range of IP and optical services already available today and also will stimulate a new

TABLE 3.9 HOW FAST IS A 100-GBPS NETWORK?

DATA	TIME TO TRANSMIT
8.5 million electronic records	1 minute
300,000 X-rays	1 minute
1.8 million e-books simultaneously downloaded	2 minute

generation of innovative services. The goal is to create an intelligent global ecosystem that will enable researchers, scientists, and others to “turn on” high-capacity network connections whenever and wherever they are needed. **Table 3.10** describes some of the projects that Internet2’s 100-Gbps network is enabling. Other initiatives involve science and engineering (advanced network applications in support of distributed lab environments, remote access to rare scientific instruments, and distributed large-scale computation and data access), health sciences and health networks (telemedicine, medical and biological research, and health education and awareness), and arts and humanities (collaborative live performances, master classes, remote auditions, and interactive performing arts education and media events).

THE FIRST MILE AND THE LAST MILE

The Internet2 project is just the tip of the iceberg when it comes to future enhancements to the Internet. In 2007, the NSF began work on the Global Environment for Network Innovations (GENI) initiative. GENI is a unique virtual laboratory for exploring future internets at scale. GENI aims to promote innovations in network science, security technologies, services, and applications. GENI is a partnership of leading

TABLE 3.10 PROJECTS BEING ENABLED BY INTERNET2’S 100-GBPS NETWORK

PROJECT	DESCRIPTION
XSEDE (Extreme Science and Engineering Discovery Environment)	XSEDE is a collection of integrated, advanced digital resources and services that enables scientists to interactively share computing resources, data, and expertise. XSEDE supports over 8,000 members of the scientific community, and 16 supercomputers. In 2013, XSEDE upgraded from a 10-Gbps network to Internet2’s 100-Gbps network. In 2016, the NSF awarded XSEDE \$110 million in funding to enable it to continue to provide advanced cyberinfrastructure resources and services to the nation’s scientists and engineers.
CloudLab	Cloud computing test beds based at the University of Utah, Clemson, and the University of Wisconsin-Madison, connected by Internet2’s 100-Gbps network. Focusing on the development of novel cloud architectures and new cloud computing applications. Enables researchers to build their own clouds and experiment with applications such as real-time disaster response and medical record security.
University of Florida	Support for Compact Muon Solenoid (CMS) experiments at CERN’s Hadron collider (contributed to discovery of the Higgs boson particle, which earned 2013 Nobel Prize).

academic centers and private corporations such as Cisco, IBM, and HP, among many others. To date, awards have been made to 83 academic/industry teams for various projects to build, integrate, and operate early prototypes of the GENI virtual laboratory (Geni.net, 2014). Between 2015 and 2017, GENI will transition from being overseen by NSF's GENI Project Office to a community governance model (Geni.net, 2016).

The most significant privately initiated (but often government-influenced) changes are coming in two areas: fiber-optic trunk line bandwidth and wireless Internet services. Fiber optics is concerned with the first mile or backbone Internet services that carry bulk traffic long distances. Wireless Internet is concerned with the last mile—from the larger Internet to the user's smartphone, tablet computer, or laptop.

Fiber Optics and the Bandwidth Explosion in the First Mile

fiber-optic cable
consists of up to hundreds of strands of glass or plastic that use light to transmit data

Fiber-optic cable consists of up to hundreds of strands of glass that use light to transmit data. It often replaces existing coaxial and twisted pair cabling because it can transmit much more data at faster speeds, with less interference and better data security. Fiber-optic cable is also thinner and lighter, taking up less space during installation. The hope is to use fiber optics to expand network bandwidth capacity in order to prepare for the expected increases in web traffic once next-generation Internet services are widely adopted.

Telecommunication firms have made substantial investments in global, national, and regional fiber optic cable systems in the last decade. For instance, Verizon has spent over \$23 billion since 2004, building and expanding its FiOS fiber-optic Internet service that can provide speeds of up to 500 Mbps, and currently has about 6.6 million FiOS customers. In 2012, Google joined the fray with Google Fiber, a 1-Gbps fiber-optic network, that is currently available in 7 cities. This installed base of fiber-optic cable represents a vast digital highway that is currently being exploited by YouTube (Google), Facebook, and other high-bandwidth applications. But despite the interest in fiber, only about 12.3% of U.S. homes had fiber connections as of 2015, a much lower percentage than a number of other countries around the world (Buckley, 2015; Richter, 2016). **Table 3.11** illustrates several optical bandwidth standards and compares them to traditional T lines.

The Last Mile: Mobile Internet Access

Fiber-optic networks carry the long-haul bulk traffic of the Internet and play an important role in bringing high-speed broadband to the household and small business. The goal of the Internet2 and GENI projects is to bring gigabit and ultimately terabit bandwidth to the household over the next 20 years. But along with fiber optics, arguably the most significant development for the Internet and Web has been the emergence of mobile Internet access.

Wireless Internet is concerned with the last mile of Internet access to the user's home, office, car, smartphone, or tablet computer, anywhere they are located. Up until 2000, the last-mile access to the Internet—with the exception of a small satellite Internet connect population—was bound up in land lines of some sort: copper coaxial TV cables or telephone lines or, in some cases, fiber-optic lines to the office. Today,

TABLE 3.11 HIGH-SPEED OPTICAL BANDWIDTH STANDARDS

STANDARD SPEED	
T1	1.544 Mbps
T3	43.232 Mbps
OC-3	155 Mbps
OC-12	622 Mbps
OC-48	2.5 Gbps
OC-192	10 Gbps
OC-768	40 Gbps

Note: "OC" stands for Optical Carrier and is used to specify the speed of fiber-optic networks conforming to the SONET standard. SONET (Synchronous Optical Networks) includes a set of signal rate multiples for transmitting digital signals on optical fiber. The base rate (OC-1) is 51.84 Mbps.

in comparison, high-speed cell phone networks and Wi-Fi network hotspots provide a major alternative.

Today, sales of desktop computers have been eclipsed by sales of smartphones and tablet and ultramobile laptop computers with built-in wireless networking functionality. Clearly, a large part of the Internet is now mobile, access-anywhere broadband service for the delivery of video, music, and web search. According to eMarketer, there are over 210 million mobile Internet users in the United States in 2016 (about 65% of the population), and almost 2.5 billion worldwide (eMarketer, Inc., 2016f).

Telephone-based versus Computer Network-based Wireless Internet Access

There are two different basic types of wireless Internet connectivity: telephone-based and computer network-based systems.

Telephone-based wireless Internet access connects the user to a global telephone system (land, satellite, and microwave) that has a long history of dealing with millions of users simultaneously and already has in place a large-scale transaction billing system and related infrastructure. Cellular telephones and the telephone industry are currently the largest providers of wireless access to the Internet today. Around 1.5 billion smartphones are expected to be sold worldwide in 2016 (Gartner, Inc., 2016b). Smartphones combine the functionality of a cell phone with that of a laptop computer with Wi-Fi capability. This makes it possible to combine in one device music, video, web access, and telephone service. Tablet computers can also access cellular networks. **Table 3.12** summarizes the various telephone technologies currently being used and under development for wireless Internet access. 5G wireless is the next frontier. Although official standards are not expected to be fully rolled out for a few years, telecommunications companies will likely start to introduce technology branded as "5G" as soon as 2017.

TABLE 3.12 WIRELESS INTERNET ACCESS TELEPHONE TECHNOLOGIES

TECHNOLOGY	SPEED	DESCRIPTION	PLAYERS
<i>3G (THIRD GENERATION)</i>			
CDMA2000 EV-DO HSPA (W-CDMA)	144 Kbps–2 Mbps	High-speed, mobile, always on for e-mail, browsing, and instant messaging. Implementing technologies include versions of CDMA2000 EV-DO (used by CDMA providers) and HSPDA (used by GSM providers). Nearly as fast as Wi-Fi.	Verizon, Sprint, AT&T, T-Mobile, Vodafone
<i>3.5G (3G+)</i>			
CDMA2000 EV-DO, Rev.B	Up to 14.4 Mbps	Enhanced version of CDMA 2000 EV-DO.	Verizon, Sprint
HSPA+	Up to 11 Mbps	Enhanced version of HSPA.	AT&T, T-Mobile
<i>4G (FOURTH GENERATION)</i>			
Long-Term Evolution (LTE)	Up to 100 Mbps	True broadband on cell phone; lower latency than previous generations.	AT&T, Verizon, Sprint, T-Mobile (in 2013)
<i>5G (FIFTH GENERATION)</i>			
Standards under development; expected by 2020	Up to 10 Gbps	Goals include 1–10 Gbps connectivity; sub-1 millisecond latency enabling services such as autonomous driving, augmented reality, virtual reality, and immersive/tactile Internet.	Ericsson, SK Telecom, Huawei, Samsung, NTT DoCoMo, Verizon, national governments

Wi-Fi

Wireless standard for Ethernet networks with greater speed and range than Bluetooth

Wireless local area network (WLAN)-based Internet access derives from a completely different background from telephone-based wireless Internet access. Popularly known as **Wi-Fi**, WLANs are based on computer local area networks where the task is to connect client computers (generally stationary) to server computers within local areas of, say, a few hundred meters. Wi-Fi functions by sending radio signals that are broadcast over the airwaves using certain radio frequency ranges (2.4 GHz to 5.875 GHz, depending on the type of standard involved). The major technologies here are the various versions of the Wi-Fi standard, WiMax, and Bluetooth (see **Table 3.13**).

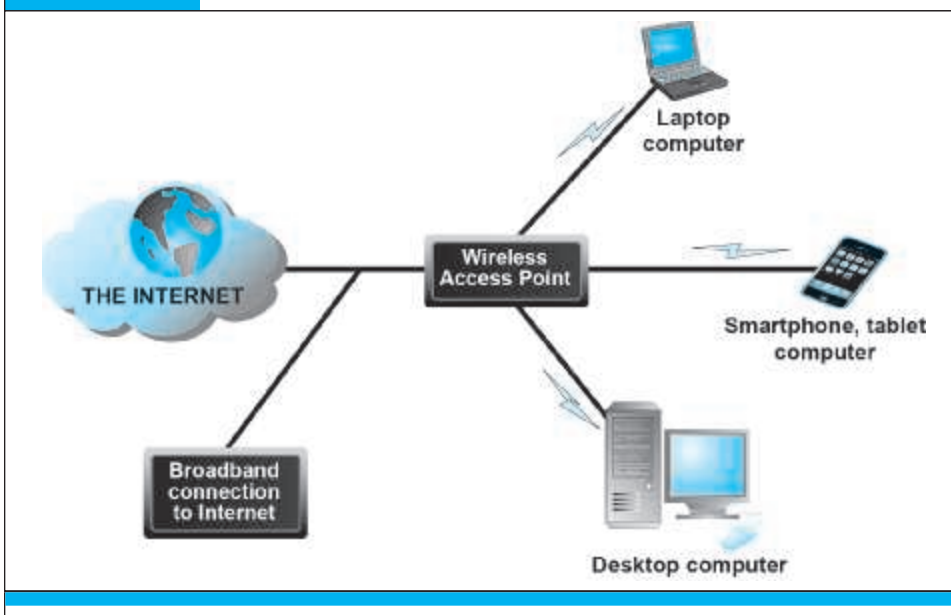
In a Wi-Fi network, a *wireless access point* (also known as a “hot spot”) connects to the Internet directly via a broadband connection (cable, DSL telephone, or T1 line) and then transmits a radio signal to a transmitter/receiver installed in a tablet or laptop computer or smartphone. **Figure 3.14** illustrates how a Wi-Fi network works.

Wi-Fi provided under the 802.11 a/b/g/n specifications offers high-bandwidth capacity from 11 Mbps up to a maximum of 7 Gbps—far greater than any 3G or 4G service currently in existence—but has a limited range of 300 meters, with the exception of WiMax discussed below. Wi-Fi is also exceptionally inexpensive. The cost of creating a corporate Wi-Fi network in a single 14-story building with an access point for each floor is less than \$100 an access point. It would cost well over \$500,000 to

TABLE 3.13 WIRELESS NETWORK INTERNET ACCESS TECHNOLOGIES

TECHNOLOGY	RANGE/SPEED	DESCRIPTION	PLAYERS
Wi-Fi (IEEE 802.11 a/b/g/n)	300 feet/11–70 Mbps	Evolving high-speed, fixed broadband wireless local area network for commercial and residential use	Linksys, Cisco, and other Wi-Fi router manufacturers; entrepreneurial network developers
802.11ac	500 Mbps–1 Gbps		
802.11ad	less than 10 meters/ up to 7 Gbps		
WiMax (IEEE 802.16)	30 miles/50–70 Mbps	High-speed, medium-range, broadband wireless metropolitan area network	Clearwire, Sprint, Fujitsu, Intel, Alcatel, Proxim
Bluetooth (wireless personal area network)	1–30 meters/1–3 Mbps	Modest-speed, low-power, short-range connection of digital devices	Sony Ericsson, Nokia, Apple, HP, and other device makers

wire the same building with Ethernet cable. IEEE 802.11ac is a version of the 802.11 specification adopted in December 2013 that provides for effective throughputs of 500 Mbps to over 1 Gbps. The newest standard, IEEE 802.11ad, provides for theoretical maximum throughput up to 7 Gbps. The first 802.11ad devices began shipping at the beginning of 2016. Next-generation Wi-Fi standards currently being worked on by

FIGURE 3.14 WI-FI NETWORKS

In a Wi-Fi network, wireless access points connect to the Internet using a land-based broadband connection. Clients, which could be desktops, laptops, tablet computers, or smartphones, connect to the access point using radio signals.

the IEEE 802.11 Working Group include 802.11ay, which deals with 60 GHz wireless operations, and will provide for data rates of up to 20 Gbps, and 802.11ax, aimed at high-efficiency WLANs used for stadiums and other areas where many people want to access a Wi-Fi network at the same time. A next-generation 802.11ah standard aimed at the Internet of Things is also being developed (Weiss, 2015; Hsu, 2015).

While initially a grass roots, “hippies and hackers” public access technology, billions of dollars have subsequently been poured into private ventures seeking to create for-profit Wi-Fi networks. One of the most prominent networks has been created by Boingo Wireless with more than 1 million hotspots around the globe. Optimum WiFi (available to Optimum Online customers for free) also offers over 1.5 million hotspots around the world. AT&T Wi-Fi Services (formerly Wayport) has another large network that provides Wi-Fi service at hotels, airports, McDonald’s, and IHOP restaurants, and Hertz airport rental offices, with thousands of hotspots throughout the United States. T-Mobile and Sprint also have nationwide Wi-Fi services at Starbucks coffee shops and thousands of other public locations. Apple, in turn, has made Wi-Fi automatically available to iPhone and iPad devices as an alternative to the more expensive and much slower 3G and 4G cellular systems. In 2015, for the first time, a majority (51%) of mobile Internet traffic originated from Wi-Fi rather than cellular systems, and it is expected that Wi-Fi will be carrying over half of all Internet traffic by 2019 (Cisco, 2016).

A second WLAN technology for connecting to the Internet, and for connecting Internet devices to one another, is called Bluetooth. **Bluetooth** is a personal connectivity technology that enables links between mobile devices and connectivity to the Internet (Bluetooth.com, 2016). Bluetooth is the universal cable cutter, promising to get rid of the tangled mess of wires, cradles, and special attachments that plague the current world of personal computing. With Bluetooth, users can wear a wireless earbud, share files in a hallway or conference room, synchronize their smartphone with their laptop without a cable, send a document to a printer, and even pay a restaurant bill from the table to a Bluetooth-equipped cash register. Bluetooth is also an unregulated media operating in the 2.4 GHz spectrum but with a very limited range of 30 feet or less. It uses a frequency hopping signal with up to 1,600 hops per second over 79 frequencies, giving it good protection from interference and interception. Bluetooth-equipped devices constantly scan their environments looking for connections to compatible devices. Today, almost all mobile devices are Bluetooth-enabled. Bluetooth may also play a role in the future as a platform for the Internet of Things (see page 152).

Bluetooth

technology standard for short-range wireless communication under 30 feet

INTERNET ACCESS DRONES

A new method of providing Internet access to areas that are not well served by wired or cellular networks is being explored by companies such as Google and Facebook. Both companies have recently purchased companies that make drones (unmanned aircraft/satellites) that may be used to provide Internet access to remote parts of the world.

In 2014, Google purchased Titan Aerospace, which makes solar-powered drones that can fly for several years at 65,000 feet. Google is reportedly experimenting with

using drones to deliver 5G wireless Internet service. Google is also experimenting with high-altitude balloons with its Project Loon. Google envisions a network of balloons circling high above the earth in the stratosphere, establishing a ring of uninterrupted connectivity. In 2014, Google sent a prototype of a networked hot-air balloon around the world in 22 days, even taking photos for its Street View program, and in 2015, the government of Sri Lanka announced that Sri Lanka would be the first country to use Project Loon to provide universal Internet access across Sri Lanka. In August 2016, Google is reportedly taking steps to move Project Loon from a research project into a profitable business.

In a similar effort, Facebook has put together the Facebook Connectivity Lab, where engineers are focusing on solar-powered drones, satellites, and infrared lasers capable of providing Internet access. To propel that effort, Facebook purchased the British company Ascenta, whose founders helped create the world's longest flying solar-powered drone. In 2016, Facebook completed a full-scale test flight of its first Internet access solar-powered drone, Aquila. Created from carbon fiber, the drone has the wingspan of a Boeing 737 but weighs less than a small car, and is designed to fly at 60,000 to 90,000 feet for up to three months at a time. It reportedly uses a laser communications system that can beam data from the sky.

THE FUTURE INTERNET

The increased bandwidth and expanded wireless network connectivity of the Internet of the future will result in benefits beyond faster access and richer communications. First-mile enhancements created by fiber-optic networks will enhance reliability and quality of Internet transmissions and create new business models and opportunities. Some of the major benefits of these technological advancements include latency solutions, guaranteed service levels, lower error rates, and declining costs. Widespread wireless access to the Internet will also essentially double or even triple the size of the online shopping marketplace because consumers will be able to shop and make purchases just about anywhere. This is equivalent to doubling the physical floor space of all shopping malls in America. We describe some of these benefits in more detail in the following sections.

Latency Solutions

One of the challenges of packet switching, where data is divided into chunks and then sent separately to meet again at the destination, is that the Internet does not differentiate between high-priority packets, such as video clips, and those of lower priority, such as self-contained e-mail messages. Because the packets cannot yet be simultaneously reassembled, the result can be distorted audio and video streams.

Differentiated quality of service (diffserv) is a technology that assigns levels of priority to packets based on the type of data being transmitted. Video conference packets, for example, which need to reach their destination almost instantaneously, receive much higher priority than e-mail messages. In the end, the quality of video and audio will skyrocket without undue stress on the network. Differential service is very controversial because it means some users may get more bandwidth than others, and potentially they may have to pay a higher price for more bandwidth.

differentiated quality of service (diffserv)

a new technology that assigns levels of priority to packets based on the type of data being transmitted

Guaranteed Service Levels and Lower Error Rates

In today's Internet, there is no service-level guarantee and no way to purchase the right to move data through the Internet at a fixed pace. Today's Internet promises only "best effort." The Internet is democratic—it speeds or slows everyone's traffic alike. In the future, it might be possible to purchase the right to move data through the network at a guaranteed speed in return for higher fees.

Declining Costs

As the Internet pipeline is upgraded, the availability of broadband service will expand beyond major metropolitan areas, significantly reducing the cost of access. More users mean lower cost, as products and technology catch on in the mass market. Higher volume usage enables providers to lower the cost of both access devices, or clients, and the service required to use such products. Both broadband and wireless service fees are expected to decline as geographic service areas increase, in part due to competition for that business.

The Internet of Things

No discussion of the future Internet would be complete without mentioning the **Internet of Things (IoT)**, also sometimes referred to as the Industrial Internet. Internet technology is spreading beyond the desktop, laptop, and tablet computer, and beyond the smartphone, to consumer electronics, electrical appliances, cars, medical devices, utility systems, machines of all types, even clothing—just about anything that can be equipped with sensors that can collect data and connect to the Internet, enabling the data to be analyzed with data analytics software.

IoT builds on a foundation of existing technologies, such as radio frequency identification (RFID) tags, and is being enabled by the availability of low-cost sensors, the drop in price of data storage, the development of "big data" analytics software that can work with trillions of pieces of data, as well as implementation of IPv6, which will allow Internet addresses to be assigned to all of these new devices. Although IoT devices don't necessarily have to be wireless, most use wireless communications technology previously discussed, such as cellular networks, Wi-Fi, Bluetooth, or other wireless protocols such as ZigBee or Z-Wave, to connect either directly or via a mobile app to the Internet (often a cloud service).

IoT technology is powering the development of "smart" connected "things"—televisions, houses, and cars, as well as wearable technology—clothing and devices like the Apple Watch, profiled in the opening case. Smart televisions that integrate directly with the Internet and can run apps have become very popular, with more than half (52%) of all U.S. Internet homes having at least one TV connected to the Internet (NPD Group Inc, 2016). Smart houses have attracted even more interest, fueled by Google's purchase of Nest Labs for \$3.2 billion in 2014. Nest Labs makes smart thermostats, home security cameras, and smoke and carbon monoxide alarms. In 2015, Nest Labs announced that it was making Nest Weave, a protocol it had developed that enables appliances, thermostats, door locks, and other devices to communicate with each other and other Nest products, available to third-party developers and manufacturers. Apple

Internet of Things (IoT)

Use of the Internet to connect a wide variety of devices, machines, and sensors

announced a smart home platform that it calls HomeKit in 2014. HomeKit is a framework and network protocol for controlling devices in the home that is programmed directly into Apple's iOS software for iPhones and iPads, and is integrated with Siri, Apple's voice-activated artificial intelligence assistant. By 2016, a number of devices had been designed specifically for use with HomeKit, such as a smart thermostat, a smart deadbolt lock, a home sensor that provides temperature, humidity, and air quality readings, and an iDevices switch that enables you to turn electronic devices on and off using Siri. Many cable companies such as Time Warner Cable, Comcast, and AT&T already offer connected home systems that include appliances and lights. All in all, the global market for smart house products is expected to grow from about \$47 billion in 2015 to over \$120 billion by 2022 (Research and Markets, 2016).

In September 2014, as discussed in the chapter-opening case, Apple introduced the Apple Watch. The Apple Watch features a fitness/activity tracker similar to offerings from Fitbit, Nike +, FuelBand, and Jawbone Up, is able to access a wide variety of apps, and also works with Apple Pay, Apple's mobile payment service. A number of other manufacturers, such as Samsung, LG, Motorola, and Swatch, have also introduced smartwatches. Wearable computing is expected to grow into a \$170 billion business by 2021.

Connected cars that have built-in Internet access have also arrived (see the *Insight on Technology* case, *Are Connected Cars the Next Hot Entertainment Vehicle?* in Chapter 2). Here too, Google and Apple are major players. In 2014, Google announced the Open Automotive Alliance, a group of leading automakers and technology companies focused on bringing the Android platform to cars. Shortly thereafter, Apple announced CarPlay, a software platform that synchronizes iPhones to the car's infotainment system. Android Auto and CarPlay-enabled vehicles began to be introduced in 2015, and have become more widely available in 2016. Connected cars are likely to be integrated with smart home initiatives in the future. Already, iControl, which provides the software underlying automated home systems from Comcast, TimeWarner, ADT, and others, has entered into a partnership with Zubie, a provider of connected car services. The next frontier on the connected car front is the self-driving car, combining IoT and artificial intelligence technologies. Many Internet technology companies, ranging from giants such as Google, Baidu (China's version of Google), Uber, and Intel to start-ups like Drive.ai and Mobileye, have jumped into the fray alongside automotive companies such as Tesla, BMW, Volvo, GM, Ford, and others, with the goal of offering self-driving, autonomous cars by 2019 or sooner.

Despite all of the IoT activity, however, interoperability remains a major concern. As with many technologies in the early stages of development, many organizations are fighting to create the standards that participants in the market will follow. The AllSeen Alliance, formed by Qualcomm in 2013 with 50 other companies, including Microsoft and Cisco, is one group that hopes to create an open source standard. Membership in the Alliance has soared since its initial founding and in 2016, it has over 200 members. Another group, the Open Connectivity Foundation (formerly the Open Interconnect Consortium), formed in 2014 by Intel, Broadcom, Dell, and others apparently not happy with the AllSeen effort, has also seen its membership soar to over 200 members. A different group, the Industrial Internet Consortium, has been formed by AT&T,

Cisco, GE, IBM, and Intel to focus on engineering standards for industrial assets. The Wolfram Connected Devices Project is aimed at developing a database of IoT devices, and currently includes more than 3,000. And as with many other types of Internet-related technology, Google with its Android operating system and Apple with AirPlay wireless streaming protocol may be trying to create their own standards.

Other concerns include security and privacy. Security experts believe that IoT devices could potentially be a security disaster, with the potential for malware being spread through a connected network, and difficulty in issuing patches to devices, leaving them vulnerable (Internet Society, 2015). Data from stand-alone smart devices can reveal much personal detail about a consumer's life, and if those devices are all ultimately interconnected, there will be little that is truly private.

Although challenges remain before the Internet of Things is fully realized, it is coming closer and closer to fruition. As of 2016, experts estimate that there are anywhere from 6.4 billion to 9 billion IoT devices (not including smartphones, tablets, or desktop computers), with some projecting as many as 100 billion connected IoT devices and global economic impact of more than \$11 trillion by 2025 (Nordstrom, 2016; Internet Society, 2015).

3.4 THE WEB

Without the Web, there would be no e-commerce. The invention of the Web brought an extraordinary expansion of digital services to millions of amateur computer users, including color text and pages, formatted text, pictures, animations, video, and sound. In short, the Web makes nearly all the rich elements of human expression needed to establish a commercial marketplace available to nontechnical computer users worldwide.

While the Internet was born in the 1960s, the Web was not invented until 1989–1991 by Dr. Tim Berners-Lee of the European Particle Physics Laboratory, better known as CERN (Berners-Lee et al., 1994). Several earlier authors—such as Vannevar Bush (in 1945) and Ted Nelson (in the 1960s)—had suggested the possibility of organizing knowledge as a set of interconnected pages that users could freely browse (Bush, 1945; Ziff Davis Publishing, 1998). Berners-Lee and his associates at CERN built on these ideas and developed the initial versions of HTML, HTTP, a web server, and a browser, the four essential components of the Web.

First, Berners-Lee wrote a computer program that allowed formatted pages within his own computer to be linked using keywords (hyperlinks). Clicking on a keyword in a document would immediately move him to another document. Berners-Lee created the pages using a modified version of a powerful text markup language called Standard Generalized Markup Language (SGML).

Berners-Lee called this language HyperText Markup Language, or HTML. He then came up with the idea of storing his HTML pages on the Internet. Remote client computers could access these pages by using HTTP (introduced earlier in Section 3.1 and described more fully in the next section). But these early web pages still appeared

as black and white text pages with hyperlinks expressed inside brackets. The early Web was based on text only; the original web browser only provided a line interface.

Information shared on the Web remained text-based until 1993, when Marc Andreessen and others at the National Center for Supercomputing Applications (NCSA) at the University of Illinois created a web browser with a graphical user interface (GUI) called Mosaic that made it possible to view documents on the Web graphically—using colored backgrounds, images, and even primitive animations. Mosaic was a software program that could run on any graphically based interface such as Macintosh, Windows, or Unix. The Mosaic browser software read the HTML text on a web page and displayed it as a graphical interface document within a GUI operating system such as Windows or Macintosh. Liberated from simple black and white text pages, HTML pages could now be viewed by anyone in the world who could operate a mouse and use a Macintosh or PC.

Aside from making the content of web pages colorful and available to the world's population, the graphical web browser created the possibility of universal computing, the sharing of files, information, graphics, sound, video, and other objects across all computer platforms in the world, regardless of operating system. A browser could be made for each of the major operating systems, and the web pages created for one system, say, Windows, would also be displayed exactly the same, or nearly the same, on computers running the Macintosh or Unix operating systems. As long as each operating system had a Mosaic browser, the same web pages could be used on all the different types of computers and operating systems. This meant that no matter what kind of computer you used, anywhere in the world, you would see the same web pages. The browser and the Web have introduced us to a whole new world of computing and information management that was unthinkable prior to 1993.

In 1994, Andreessen and Jim Clark founded Netscape, which created the first commercial browser, **Netscape Navigator**. Although Mosaic had been distributed free of charge, Netscape initially charged for its software. In August 1995, Microsoft Corporation released its own free version of a browser, called **Internet Explorer**. In the ensuing years, Netscape fell from a 100% market share to less than .5% in 2009. The fate of Netscape illustrates an important e-commerce business lesson. Innovators usually are not long-term winners, whereas smart followers often have the assets needed for long-term survival. Much of the Netscape browser code survives today in the Firefox browser produced by Mozilla, a nonprofit heavily funded by Google.

HYPertext

Web pages can be accessed through the Internet because the web browser software on your PC can request web pages stored on an Internet host server using the HTTP protocol. Hypertext is a way of formatting pages with embedded links that connect documents to one another and that also link pages to other objects such as sound, video, or animation files. When you click on a graphic and a video clip plays, you have clicked on a hyperlink. For example, when you type a web address in your browser such as <http://www.sec.gov>, your browser sends an HTTP request to the sec.gov server requesting the home page of sec.gov.

Mosaic

Web browser with a graphical user interface (GUI) that made it possible to view documents on the Web graphically

universal computing

the sharing of files, information, graphics, sound, video, and other objects across all computer platforms in the world, regardless of operating system

Netscape Navigator

the first commercial web browser

Internet Explorer

Microsoft's web browser

hypertext

a way of formatting pages with embedded links that connect documents to one another, and that also link pages to other objects such as sound, video, or animation files

HTTP is the first set of letters at the start of every web address, followed by the domain name. The domain name specifies the organization's server computer that is housing the document. Most companies have a domain name that is the same as or closely related to their official corporate name. The directory path and document name are two more pieces of information within the web address that help the browser track down the requested page. Together, the address is called a Uniform Resource Locator, or URL. When typed into a browser, a URL tells it exactly where to look for the information. For example, in the following URL:

`http://www.megacorp.com/content/features/082602.html`

`http` = the protocol used to display web pages

`www.megacorp.com` = domain name

`content/features` = the directory path that identifies where on the domain web server the page is stored

`082602.html` = the document name and its format (an HTML page)

The most common domain extensions (known as general top-level domains, or gTLDs) currently available and officially sanctioned by ICANN are shown in **Table 3.14**. Countries also have domain names, such as .uk, .au, and .fr (United Kingdom, Australia, and France, respectively). These are sometimes referred to as country-code top-level domains, or ccTLDs. In 2008, ICANN approved a significant expansion of gTLDs, with potential new domains representing cities (such as .berlin), regions (.africa), ethnicity (.eus), industry/activities (such as .health), and even brands (such as .deloitte). In 2009, ICANN began the process of implementing these guidelines. In 2011, ICANN removed nearly all restrictions on domain names, thereby greatly expanding the number of different domain names available. As of August 2016, over 1,150 gTLDs have been applied for, acquired, and launched. The new gTLDs are in multiple languages and scripts/characters (including Arabic, Chinese, Japanese, and Russian) and include geographic place names such as .nyc, .london, and .paris; business identifiers such as .restaurant, .realtor, .technology, and .lawyer; brand names such as .bmw and .suzuki; and a whole host of other descriptive names.

ICANN: Internet Corporation for Assigned Names and Numbers

MARKUP LANGUAGES

Although the most common web page formatting language is HTML, the concept behind document formatting actually had its roots in the 1960s with the development of Generalized Markup Language (GML).

HyperText Markup Language (HTML)

HyperText Markup Language (HTML) is a GML that is relatively easy to use. HTML provides web page designers with a fixed set of markup "tags" that are used to format a web page (see **Figure 3.15**). When these tags are inserted into a web page, they are read by the browser and interpreted into a page display. You can see the source HTML

HyperText Markup Language (HTML)

GML that is relatively easy to use in web page design. HTML provides web page designers with a fixed set of markup "tags" that are used to format a web page

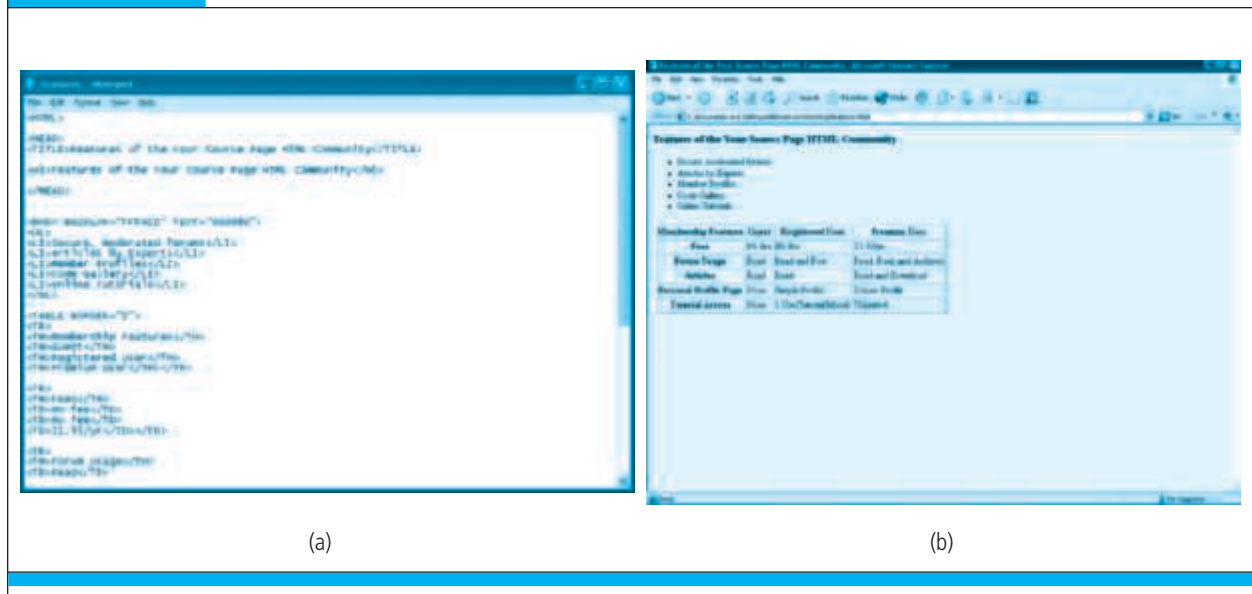
TABLE 3.14 **EXAMPLES OF TOP-LEVEL DOMAINS**

GENERAL TOP-LEVEL DOMAIN (GTLD)	YEAR(S) INTRODUCED	PURPOSE	SPONSOR/ OPERATOR
.com	1980s	Unrestricted (but intended for commercial registrants)	VeriSign
.edu	1980s	U.S. educational institutions	Educause
.gov	1980s	U.S. government	U.S. General Services Administration
.mil	1980s	U.S. military	U.S. Department of Defense Network Information Center
.net	1980s	Unrestricted (but originally intended for network providers, etc.)	VeriSign
.org	1980s	Unrestricted (but intended for organizations that do not fit elsewhere)	Public Interest Registry (was operated by VeriSign until December 31, 2002)
.int	1998	Organizations established by international treaties between governments	Internet Assigned Numbers Authority (IANA)
.aero	2001	Air-transport industry	Société Internationale de Telecommunications Aeronautiques SC (SITA)
.biz	2001	Businesses	NeuLevel
.coop	2001	Cooperatives	DotCooperation LLC
.info	2001	Unrestricted use	Afilias LLC
.museum	2001	Museums	Museum Domain Name Association (MuseDoma)
.name	2001	For registration by individuals	Global Name Registry Ltd.
.pro	2002	Accountants, lawyers, physicians, and other professionals	RegistryPro Ltd
.jobs	2005	Job search	Employ Media LLC
.travel	2005	Travel search	Tralliance Corporation
.mobi	2005	Websites specifically designed for mobile phones	mTLD Top Level Domain, Ltd.
.cat	2005	Individuals, organizations, and companies that promote the Catalan language and culture	Fundació puntCAT
.asia	2006	Regional domain for companies, organizations, and individuals based in Asia	DotAsia Organization
.tel	2006	Telephone numbers and other contact information	ICM Registry
.xxx	2010	New top-level domain for pornographic content	None yet approved

SOURCE: Based on data from ICANN, 2011b.

FIGURE 3.15

EXAMPLE HTML CODE (A) AND WEB PAGE (B)



HTML is a text markup language used to create web pages. It has a fixed set of “tags” that are used to tell the browser software how to present the content on screen. The HTML shown in Figure 3.15 (a) creates the web page seen in Figure 3.15 (b).

SOURCES: (A) Notepad, Microsoft Windows, Microsoft Corporation; (B) Internet Explorer, Microsoft Windows, Microsoft Corporation.

code for any web page by simply clicking on the “Page Source” command found in all browsers. In Figure 3.15, the HTML code in the first screen produces the display in the second screen.

HTML defines the structure and style of a document, including the headings, graphic positioning, tables, and text formatting. Since its introduction, the major browsers have continuously added features to HTML to enable programmers to further refine their page layouts. Unfortunately, some browser enhancements may work only in one company’s browser. Whenever you build an e-commerce site, you should take care that the pages can be viewed by the major browsers, even outdated versions of browsers. HTML web pages can be created with any text editor, such as Notepad or WordPad, using Microsoft Word (simply save the Word document as a web page), or any one of several web page development tools such as Microsoft Expression Web or Adobe Dreamweaver CC.⁵

The most recent version of HTML is HTML5. HTML5 introduces features like video playback and drag-and-drop that in the past were provided by plug-ins like Adobe Flash. HTML5 is also used in the development of mobile websites and mobile apps, and is an important tool in both responsive web design and adaptive web delivery, all of which are discussed more fully in Chapter 4. The *Insight on Technology* case, *The Rise of HTML5*, examines the increasing use of HTML5.

⁵ A detailed discussion of how to use HTML is beyond the scope of this text.

INSIGHT ON TECHNOLOGY

THE RISE OF HTML5

In 2010, Apple founder Steve Jobs lambasted Adobe Flash for its poor security, poor performance on mobile devices, and for being an energy hog.

Jobs instead trumpeted HTML5 as the preferred method for displaying video online. Fast forward to 2016. Two years after its official ratification by the W3C, the Web's standards-setting organization, HTML5 has become a de facto standard, proving once again Jobs' uncanny ability to see and perhaps shape the future.

HTML5 has become a catch-all term that encompasses not only the video element but also the use of the newest versions of Cascading Style Sheets (CSS3) and JavaScript, and another new tool, HTML5 Canvas, that is used with a set of JavaScript functions to render simple animations, which reduces page load time. HTML5 provides not only device independence, but can also access the built-in functionality of mobile devices, such as GPS and swiping, enabling the creation of web-based mobile apps that can replicate the native app experience. Web-based mobile apps (HTML5 apps) work just like web pages, with page content, including graphics, images, and video, loaded into the browser from a web server, rather than residing in the mobile device hardware like a native app. This concept has been embraced by mobile developers who naturally dream of being able to reach all platforms with a single product.

For businesses, the cost savings of HTML5 are obvious. A single HTML5 app requires far less effort to build than multiple native apps for the iOS, Android, Windows Phone, and other platforms. HTML5 apps can more easily be linked to and shared on social networks, encouraging viral distribution. Some HTML5 apps can even be designed so that they can be run on mobile devices when they are offline. Differences in how apps run across different platforms and workarounds are eliminated.

In the past, HTML5 apps couldn't approach the smooth and speedy user experience of a native app, but thanks to advancements in the underlying technologies behind HTML5 and improvements in the expertise of HTML5 developers, that is no longer the case. Flash also requires installation, whereas HTML5 does not.

In 2014, the Interactive Advertising Bureau (IAB), together with a number of the largest online publishers and advertising firms, urged advertisers to implement HTML5 as the standard for mobile ads in order to guarantee that ads will run and look good on different platforms, and in 2015 released guidelines that fully embrace HTML5, citing interoperability and the improved effectiveness of HTML5 ads. The rise of HTML5 has mirrored the growth of the mobile platform as it supplants Flash, which was developed for the desktop, as the preferred media delivery platform on the Web. During this time, Flash has continued to struggle with critical security vulnerabilities. In response, the online advertising industry has responded by reducing or eliminating the use of Flash. For instance, in 2016, Facebook mandated HTML5 instead of Flash for all videos posted to its site, reporting improved loading times, fewer bugs, and better engagement, and Google signaled a shift towards HTML5 by blocking Flash advertisements from autoplaying in Chrome, in part due to their notorious security issues. In 2016, Chrome began to automatically block any non-visible Flash content, like tracking cookies, and by year's end, HTML5 will be the "default" for Chrome, except where sites only support Flash. Google also announced that its display ads would be 100 percent HTML5 by the beginning of 2017. Mozilla Firefox made a similar announcement shortly thereafter regarding non-visible Flash content and its own plans to make HTML5 its default by 2017, meaning that over 80% of the web browser market is now blocking Flash. Apple's

(continued)



Safari browser, one of the first to impose restrictions on Flash, has taken steps to prevent sites offering both Flash and HTML5 from displaying Flash content. Twitch, one of the largest sites still using Flash video streaming, announced it would begin a switch to HTML5 in 2016, just as YouTube did a year earlier. The moves from these advertising and tech juggernauts have solidified the downfall of Flash and the rise of HTML5 as the future of advertising. Even Adobe itself has begun to recommend that content creators use HTML5 instead of Flash and has renamed its Flash Professional tool to 'Adobe Animate CC,' adding HTML5 support and the ability to convert Flash advertisements to HTML5.

Retailers have taken notice. One example of a company using HTML5 with success is Rakuten Shopping, an online retailer that offers a wide variety of goods online, and is currently ranked as one of Internet Retailer's top 30 mobile retailers. Using HTML5 has enabled Rakuten to shift away from using cookies to store customer attributes and has lightened the load on its servers.

Another example is the *Financial Times*, whose HTML5 app has proven to be an important driver for FT's business. FT first switched from a native app to HTML5 in 2011, in part to make maintaining the app across multiple platforms and devices easier. In 2013, FT rolled out a redesign of the app, featuring even more videos and personalization features.

In fact, according to Indeed, which searches millions of jobs from thousands of different job

sites, "HTML5" continues to be one of the fastest growing keywords found in online job postings. Many online advertisers that have relied heavily on Flash are also struggling to adapt to the emergence of HTML5 ads, which are larger in size and require testing on more platforms. Content creators and advertisers alike are also uneager to manage two different formats. In the past, they only had to deal with Flash, and many have been unwilling to make the transition just yet.

However, even given all its benefits, HTML5 is not without flaws. For instance, HTML5 has not consistently supported digital rights management (DRM). In the past, media companies developed their own copy protection standards based on geographical region and/or whether payment had been proffered. These were enforced through their own media players. Because HTML5 does not require plug-ins to play video (or audio), and further, because HTML5 is an official W3C standard charged with remaining vendor neutral, this presents a challenge to HTML5 developers. HTML5 also allows websites to track how much battery power their site visitors have remaining. This feature was implemented so that sites could warn users to recharge their battery, but the reporting is so detailed that sites can determine what sites you've come from last solely based on your battery information, presenting privacy concerns. However, the security issues with HTML5 pale in comparison to those associated with Flash, and it's still early in the development cycle for HTML5.

SOURCES: "Google Nixes Flash, Embraces HTML5 in Chrome Browser," by Paul Krill, Infoworld.com, August 11, 2016; "Publishers Must Embrace Transition From Flash to HTML5 Before It's Too Late," by Brian DeFrancesco, Publishersdaily.com, August 5, 2016; "Firefox Sets Kill-Flash Schedule," by Gregg Keizer, Infoworld.com, July 22, 2016; "Twitch Begins Shift from Flash to HTML5 with Closed Beta," by Devin Coldevey, Techcrunch.com, July 14, 2016; "Safari 10 To Turn Off Flash by Default," by John Ribeiro, Infoworld.com, June 15, 2016; "As Flash Apocalypse Approaches, Here are HTML5 Rules of Thumb to Keep in Mind," by Barry Levine, Marketingland.com, May 26, 2016; "Facebook's Website Now Uses HTML5 Instead of Flash for All Videos," by Chris Welch, Theverge.com, December 18, 2015; "Why We Chose to Move to HTML5 Video," by Daniel Baulig, Code.facebook.com, December 18, 2015; "Adobe Tells Developers to Use HTML5 Instead of Flash," by Fahmida Y. Rashid, Infoworld.com, December 2, 2015; "Adobe Bows to HTML5 and Renames Its Flash Professional App," by Steve Dent, Engadget.com, December 1, 2015; "Transforming the Web with HTML5," by Christina Mulligan, Sdtimes.com, October 5, 2015; "With Digital Ads Shifting to HTML5, the Industry Now Has a New Set of Guidelines," by Christopher Heine, Adweek.com, September 28, 2015; "HTML5 Looks Good in Light of Google, Facebook and IAB Moves," by Carl Weinschenk, September 22, 2015; "How Your Smartphone's Battery Life Can Be Used to Invade Your Privacy," by Alex Hern, *The Guardian*, August 4, 2015; "RIP Flash: Why HTML5 Will Finally Take Over Video and the Web This Year," by Erika Trautman, Thenextweb.com, April 19, 2014; "Financial Times: There Is No Drawback to Working in HTML5," by Stuart Dredge, Theguardian.com, April 29, 2013; "Adobe's Flash Surrender Proves Steve Jobs and Apple Were Right All Along with HTML5," by Nigam Arora, *Forbes*, November, 9, 2011.

FIGURE 3.16 A SIMPLE XML DOCUMENT

```
<?xml version="1.0"?>
<note>
<to>George</to>
<from>Carol</from>
<heading>Just a Reminder</heading>
<body>Don't forget to order the groceries from FreshDirect!</body>
</note>
```

The tags in this simple XML document, such as `<note>`, `<to>`, and `<from>`, are used to describe data and information, rather than the look and feel of the document.

eXtensible Markup Language (XML)

eXtensible Markup Language (XML) takes web document formatting a giant leap forward. XML is a markup language specification developed by the W3C that is similar to HTML, but has a very different purpose. Whereas the purpose of HTML is to control the “look and feel” and display of data on the web page, XML is designed to describe data and information. For example, consider the sample XML document in **Figure 3.16**. The first line in the sample document is the XML declaration, which is always included; it defines the XML version of the document. In this case, the document conforms to the 1.0 specification of XML. The next line defines the first element of the document (the root element): `< note >`. The next four lines define four child elements of the root (`to`, `from`, `heading`, and `body`). The last line defines the end of the root element. Notice that XML says nothing about how to display the data, or how the text should look on the screen. HTML is used for information display in combination with XML, which is used for data description.

Figure 3.17 shows how XML can be used to define a database of company names in a company directory. Tags such as `< Company >`, `< Name >`, and `< Specialty >` can be defined for a single firm, or an entire industry. On an elementary level, XML is extraordinarily easy to learn and is very similar to HTML except that you can make up your own tags. At a deeper level, XML has a rich syntax and an enormous set of software tools, which make XML ideal for storing and communicating many types of data on the Web.

XML is “extensible,” which means the tags used to describe and display data are defined by the user, whereas in HTML the tags are limited and predefined. XML can also transform information into new formats, such as by importing information from a database and displaying it as a table. With XML, information can be analyzed and displayed selectively, making it a more powerful alternative to HTML. This means that business firms, or entire industries, can describe all of their invoices, accounts payable, payroll records, and financial information using a web-compatible markup language. Once described, these business documents can be stored on intranet web servers and shared throughout the corporation.

Really Simple Syndication (RSS) is an XML format that allows users to have digital content, including text, articles, blogs, and podcast audio files, automatically

eXtensible Markup Language (XML) a markup language specification developed by the World Wide Web Consortium (W3C) that is designed to describe data and information

Really Simple Syndication (RSS)

program that allows users to have digital content, including text, articles, blogs, and podcast audio files, automatically sent to their computers over the Internet

FIGURE 3.17 SAMPLE XML CODE FOR A COMPANY DIRECTORY

```

<?xml version="1.0"?>
<Companies>
  <Company>
    <Name>Azimuth Interactive Inc.</Name>
    <Specialties>
      <Specialty>HTML development</Specialty>
      <Specialty>technical documentation</Specialty>
      <Specialty>ROBO Help</Specialty>
    </Specialties>
    <Country>United States</Country>
  </Company>
  <Company>
    ...
  </Company>
  ...
</Companies>

```

This XML document uses tags to define a database of company names.

sent to their computers over the Internet. An RSS aggregator software application that you install on your computer gathers material from the websites and blogs that you tell it to scan and brings new information from those sites to you. Sometimes this is referred to as “syndicated” content because it is distributed by news organizations and other syndicators (or distributors). Users download an RSS aggregator and then “subscribe” to the RSS “feeds.” When you go to your RSS aggregator’s page, it will display the most recent updates for each channel to which you have subscribed. RSS has rocketed from a “techie” pastime to a broad-based movement. Although Google has closed down Google Reader, a popular RSS product, a number of other RSS reader options remain, including Feedly, Reeder, and NewsBlur.

web server is a computer system that hosts websites (web pages).

web server software

software that enables a computer to deliver web pages written in HTML to client computers on a network that request this service by sending an HTTP request

WEB SERVERS AND CLIENTS

We have already described client/server computing and the revolution in computing architecture brought about by client/server computing. **You already know that a server is a computer attached to a network that stores files, controls peripheral devices, interfaces with the outside world—including the Internet—and does some processing for other computers on the network.**

But what is a **web server**? **Web server software** refers to the software that enables a computer to deliver web pages written in HTML to client computers on a network that request this service by sending an HTTP request. **Apache**, which works with **Linux** and **Unix** operating systems, is the most commonly used type of **web server software**. Microsoft’s **Internet Information Services (IIS)** also has significant market share (Netcraft, 2016).

Terminal

1

3 NGINX

Aside from responding to requests for web pages, all web servers provide some additional basic capabilities such as the following:

- **Security services**—These consist mainly of authentication services that verify that the person trying to access the site is authorized to do so. For websites that process payment transactions, the web server also supports SSL and TLS, the protocols for transmitting and receiving information securely over the Internet. When private information such as names, phone numbers, addresses, and credit card data needs to be provided to a website, the web server uses SSL to ensure that the data passing back and forth from the browser to the server is not compromised.
- **FTP**—This protocol allows users to transfer files to and from the server. Some sites limit file uploads to the web server, while others restrict downloads, depending on the user's identity.
- **Search engine**—Just as search engine sites enable users to search the entire Web for particular documents, search engine modules within the basic web server software package enable indexing of the site's web pages and content and permit easy keyword searching of the site's content. When conducting a search, a search engine makes use of an index, which is a list of all the documents on the server. The search term is compared to the index to identify likely matches.
- **Data capture**—Web servers are also helpful at monitoring site traffic, capturing information on who has visited a site, how long the user stayed there, the date and time of each visit, and which specific pages on the server were accessed. This information is compiled and saved in a log file, which can then be analyzed. By analyzing a log file, a site manager can find out the total number of visitors, the average length of each visit, and the most popular destinations, or web pages.

The term *web server* is also used to refer to the physical computer that runs web server software. Leading manufacturers of web server computers include Lenovo, Dell, and Hewlett-Packard. Although any desktop computer can run web server software, it is best to use a computer that has been optimized for this purpose. To be a web server, a computer must have the web server software installed and be connected to the Internet. Every public web server computer has an IP address. For example, if you type `http://www.pearsonhighered.com/laudon` in your browser, the browser software sends a request for HTTP service to the web server whose domain name is `pearsonhighered.com`. The server then locates the page named “laudon” on its hard drive, sends the page back to your browser, and displays it on your screen. Of course, firms also can use web servers for strictly internal local area networking in intranets.

Aside from the generic web server software packages, there are actually many types of specialized servers on the Web, from **database servers** that access specific information within a database, to **ad servers** that deliver targeted banner ads, to **mail servers** that provide e-mail messages, and **video servers** that provide video clips. At a small e-commerce site, all of these software packages might be running on a single computer, with a single processor. At a large corporate site, there may be hundreds or thousands of discrete server computers, many with multiple processors, running specialized web server functions. We discuss the architecture of e-commerce sites in greater detail in Chapter 4.

database server

server designed to access specific information within a database

ad server

server designed to deliver targeted banner ads

mail server

server that provides e-mail messages

video server

server that serves video clips

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

office.com and then sign in

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

1

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

2

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

3

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).

4

It is small and fast and offers many features such as pop-up blocking and tabbed

5

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.

6

3.5 THE INTERNET AND THE WEB: FEATURES AND SERVICES

generate

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

1

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.

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.

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.

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).

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

attachment

a file inserted within an e-mail message

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

- Traditional Desktop IM System.
- Cell Phone Short Messages
- Mobile messaging apps

online message board

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

Online Message Boards المنديات

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

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.

Voice over Internet Protocol (VoIP)

protocol that allows for transmission of voice and other forms of audio communication over the Internet

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

2

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%.

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

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

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 Official 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.”

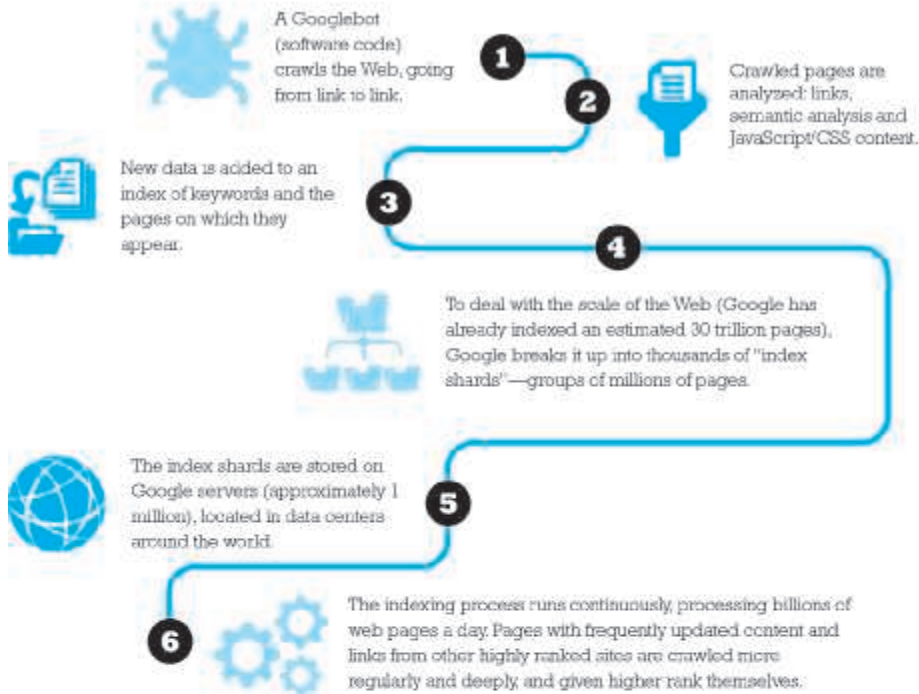
When users enter a search term at Google, Bing, Yahoo, or any of the other websites serviced by these search engines, they receive two types of listings: sponsored links, for which advertisers have paid to be listed (usually at the top of the search results page), and unsponsored “organic” search results. 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

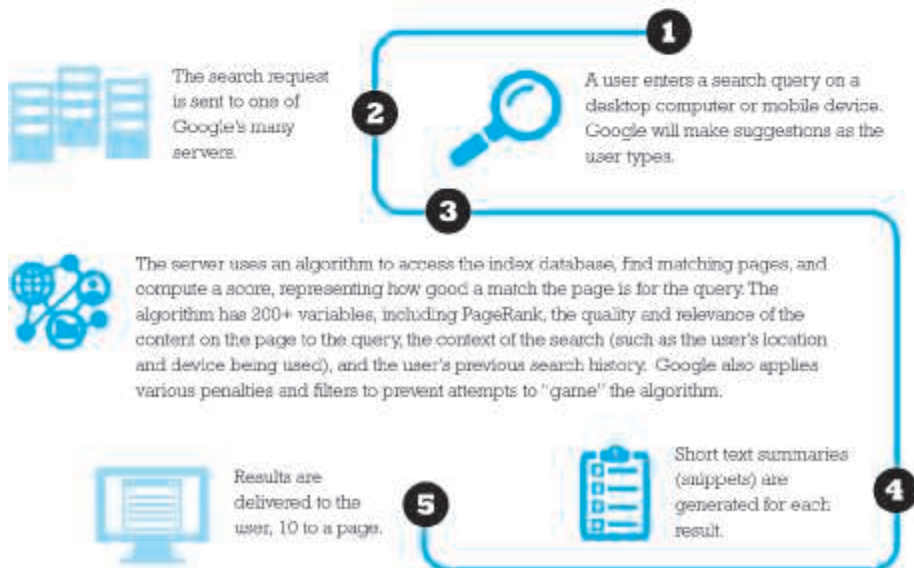
FIGURE 3.18

HOW GOOGLE WORKS

(A) Indexing the Web



(B) Processing a Search Query



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

3

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

3

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.

Generated contents

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

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

blog

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

- a kind of website or part of a website.
 - has a regularly published contents.
 - invites interactions.
 - organizes contents in reverse orders.

website vs. Blogs

A website:

- may not be expected to have fresh content.
 - may not be open to comments.
 - can contain evergreen content.
 - can have limited content that gives basic information about something.

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

wikipedia

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

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

wiki

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

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

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 experimenting 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

Situational awareness is being aware of what is happening around you in terms of where you are, where you are supposed to be, and whether anyone or anything around you is a threat to your health and safety.

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



CHAPTER

5

E-commerce Security and Payment Systems

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Understand the scope of e-commerce crime and security problems, the key dimensions of e-commerce security, and the tension between security and other values.
- Identify the key security threats in the e-commerce environment.
- Describe how technology helps secure Internet communications channels and protect networks, servers, and clients.
- Appreciate the importance of policies, procedures, and laws in creating security.
- Identify the major e-commerce payment systems in use today.
- Describe the features and functionality of electronic billing presentment and payment systems.

countries like Denmark, the Netherlands, Estonia, and tiny Belarus are building their arsenals. Unlike nuclear weapons, cyberwar is so inexpensive that even small nations can afford it. A recent report documented 29 countries with formal military and intelligence units dedicated to offensive cyberwar, 49 that have purchased off-the-shelf hacking software, and 63 currently engaged in electronic surveillance of their own and other populations. Countries are developing cyberarsenals that include collections of malware for penetrating industrial, military, and critical civilian infrastructure controllers, e-mail lists and text for phishing attacks on important targets, and algorithms for denial of service (DoS) attacks. The computer code has been tested and ready to go for offensive purposes to surprise and cripple enemy systems.

Cyberattacks on information systems have also been on the rise over the past few years. Such attacks, while not real cyberwar in the sense of incapacitating infrastructure, nevertheless illustrate the ease with which corporate and government systems can be penetrated. Some of these attacks were likely undertaken by nation states that were practicing their offensive techniques. For instance, in 2014, Sony Pictures' computer system was hacked, revealing information on 47,000 individuals, much of it e-mail correspondence among executives. About 70% of the firm's computers were incapacitated, and confidential e-mails were published by the hackers in an effort to embarrass executives of the firm. North Korea remains a major suspect, although North Korean officials denied this. In the biggest attack on U.S. government systems thus far, in July 2015, the White House announced that the Office of Personnel Management, the government's human resources agency and database, had been hacked and complete records on over 21 million people were copied, including the names of people in the defense sector. The likely source of the hack was the Chinese government. In 2016, U.S. intelligence agencies have reportedly expressed suspicions that the hacks into various e-mail accounts of Democratic National Committee officials and others associated with the Clinton campaign have been part of an orchestrated campaign by Russia to influence the 2016 presidential race. The Russian government has denied any involvement.

Attacks against physical infrastructure have been less frequent. Infrastructure attacks require detailed knowledge of the infrastructure, which usually requires insider knowledge of industrial controllers (computers that control valves and machines). The most well-known and best documented infrastructure attack was Stuxnet, malware allegedly created by Israeli and American intelligence services in 2010 in an effort to cripple thousands of Iranian nuclear centrifuges. Stuxnet was a malware virus program planted in industrial controller modules of Iranian nuclear fuel centrifuges, causing them to destroy themselves. Stuxnet was precedent-setting: it was the first large-scale cyberattack on infrastructure. In response, the Iranian government sponsored a cyberattack against the Saudi-Aramco company using a virus called Shamoon that wiped out 30,000 computers at the company. More recently, Russian hackers, allegedly employed by the Russian government, have picked up the spirit of Stuxnet and have targeted oil and gas firms. Using a "watering hole attack," the hackers launched a massive e-mail campaign to employees of these firms in an attempt to trick them into visiting a website where malware can be downloaded to their computers. While the emphasis of the attackers has been industrial

SOURCES: "Cyber Warfare: Who Is China Hacking Now?," by Kristie Lu Stout, Cnn.com, September 29, 2016; "Hacking the US Election: How the Worlds of Cyberwarfare and Politics are Colliding Spectacularly," by Kalev Leetaru, Forbes.com, September 11, 2016; "Governments and Nation States Are Now Officially Training for Cyberwarfare: An Inside Look," by Steve Ranger, Techrepublic.com, September 2, 2016; "How America Could Go Dark," by Rebecca Smith, *Wall Street Journal*, July 14, 2016; "NATO Recognizes Cyberspace as New Frontier in Defense," by Julian Barnes, *Wall Street Journal*, June 14, 2016; "'Dark Territory: The Secret History of Cyber War,'" by Fred Kaplan, by P.W. Singer, *New York Times*, March 1, 2016; "Gen. Michael Hayden Gives an Update on the Cyberwar," *Wall Street Journal*, Feb. 9, 2016; "Pentagon Chief: 2017 Budget Includes \$7B for Cyber," by Sean Lyngaas, Fcw.com, February 2, 2016; "The First Cyber Battle of the Internet of Things May Have Just Happened," by Kalev Leetaru, Forbes.com, January 5, 2016; "Ukraine: Cyberwar's Hottest Front," by Margaret Coker and Paul Sonne, *Wall Street Journal*, November 9, 2015; *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*, by Brian M. Mazanc, Potomac Books (November 1, 2015); "Cyberwar Ignites a New Arms Race," by Damian Paletta, Danny Yardon, and Jennifer Valentino-Devries, *Wall Street Journal*, October 11, 2015; "Cataloging the World's Cyberforces," by Jennifer Valentino-Devries and Danny Yardon, *Wall Street Journal*, October 11, 2015; "Obama and Xi Jinping of China Agree to Steps on Cybertheft," by Julie Davis and David Sanger, *New*

espionage, the same software could be used in a cyberwar attack against oil and gas production and transmission facilities just like the Stuxnet software that crippled Iranian nuclear centrifuges. Other infrastructure attacks include weapons known as Flame, which is thought to have caused Iran to disconnect its oil terminals from the Internet, and Snake, a malware tool kit believed to be from Russia that infected many Ukrainian civilian and industrial computer systems and networks. Snake gives attackers full access to remote systems, acts as a two-way conduit that can siphon information from systems, and provides a path for installing additional malware. Using these cyberweapons, Russia has led a three-year campaign against Ukrainian infrastructure and government systems, most recently in December 2015, when power was lost across multiple cities in Western Ukraine.

Security analysts believe the United States has developed the most powerful cyberwarfare defense and offense capabilities in the world. U.S. efforts are concentrated in the United States Cyber Command located in Fort Meade, Maryland. USCYBERCOM's stated mission is to coordinate and direct the operations and defense of Department of Defense (DoD) information networks and to prepare for military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace, and deny the same to adversaries. In early 2016, the DoD detailed a \$35 billion five-year cyberbudget aimed at furthering DoD's network defenses, building more cybertraining ranges for its cyberwarriors, and developing cybertools and infrastructure to provide offensive cyberweapons.

A number of diplomatic efforts have been undertaken by American planners to reach some sort of understanding with its cyberenemies that would set limits on cyberwar and prevent civilian casualties. These efforts are similar to nuclear arms treaties. In 2015, the Pentagon announced a new cyberstrategy outlining the conditions under which the United States would engage in a cyberweapons attack on an adversary. Routine attacks against companies will be defended by companies themselves, but attacks on U.S. government systems, infrastructure systems, defense systems, and intelligence systems that involve significant loss of life, destruction of property, or lasting economic damage, will be grounds for launching a major counterattack that will threaten similar losses to the enemy. This new policy is aimed at Russia, China, Iran, and North Korea, each of whom have been implicated in state-sponsored attacks on U.S. government and corporate systems for several years. Announcing this new policy raises the potential cost of hacking critical American systems, and is the beginning of a deterrence strategy based on the concept of mutual assured destruction.

In September 2015, the Obama administration finally reached an understanding with Chinese leaders. The presidents of both countries announced their pledge to refrain from computer-enabled theft of intellectual property for commercial gain, and attacks on their country's critical infrastructure, but there was no agreement to limit the use of cybertools for traditional espionage. A pledge is hardly a commitment and is certainly not a treaty. There is no verification protocol to ensure compliance. Nevertheless, this was the first agreement of any kind expressing the goal of restraining cyberwarfare, and since then, it appears that China has shifted its cyberespionage focus away from the United States and Western organizations to other areas of the world.

York Times, September 25, 2015; "U.S. and China Seek Arms Deal for Cyberspace," by David Sanger, *New York Times*, September 19, 2015; "Cyberthreat Posed by China and Iran Confounds White House," by David Sanger, *New York Times*, September 15, 2015; "U.S. vs. Hackers: Still Lopsided Despite Years of Warnings and a Recent Rush," by Michael Shear and Nicole Perloth, *New York Times*, July 18, 2015; "Hacking of Government Computers Exposes 21.5 Million People," by Julie Hirschfield, *New York Times*, July 9, 2015; "Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning," Government Accountability Office, July 2015; "Here's What a Cyber Warfare Arsenal Might Look Like," by Larry Greenemeier, *Scientific American*, May 6, 2015; "Pentagon Announces New Strategy for Cyberwarfare," by David Sanger, *New York Times*, April 23, 2015; "Deterrence Will Keep Lid on Cyberwar, Former Spy Chief Says," by Tim Hornyak, *Computerworld.com*, April 14, 2015; "Document Reveals Growth of Cyberwarfare Between the U.S. and Iran," by David Sanger, *New York Times*, February 22, 2015; "NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack," by David Sanger, *New York Times*, August 31, 2014; "Chinese Hackers Extending Reach to Smaller U.S. Agencies, Officials Say," by Michael Schmidt, *New York Times*, July 15, 2014; "Chinese Hackers Pursue Key Data on U.S. Workers," by Michael Schmidt, David Sanger, and Nicole Perloth, *New York Times*, July 9, 2014; "Russian Hackers Targeting Oil and Gas Companies," by Nicole Perloth, *New York Times*, June 30, 2014; "2nd China Army Unit Implicated in Online Spying," by Nicole Perloth, *New York Times*, June 9, 2014; "5 in China Army Face U.S. Charges of Cyberattacks," by Michael Schmidt and David Sanger, *New York Times*, May 19, 2014; "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government," by David Sanger and Steven Erlanger, *New York Times*, March 8, 2014.

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

profitable

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).

اختراق

Why

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 date, 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 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. محتال

although 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.

What are the steps a company can take to reduce cybercriminal activity from within a business?

not working 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 الأبعاد الرئيسية لأمن التجارة الإلكترونية

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

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 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 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 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.

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.

security breaches

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

nonrepudiation

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

authenticity الموثوقية

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

confidentiality السرية

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

privacy الخصوصية

the ability to control the use of information about oneself

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.

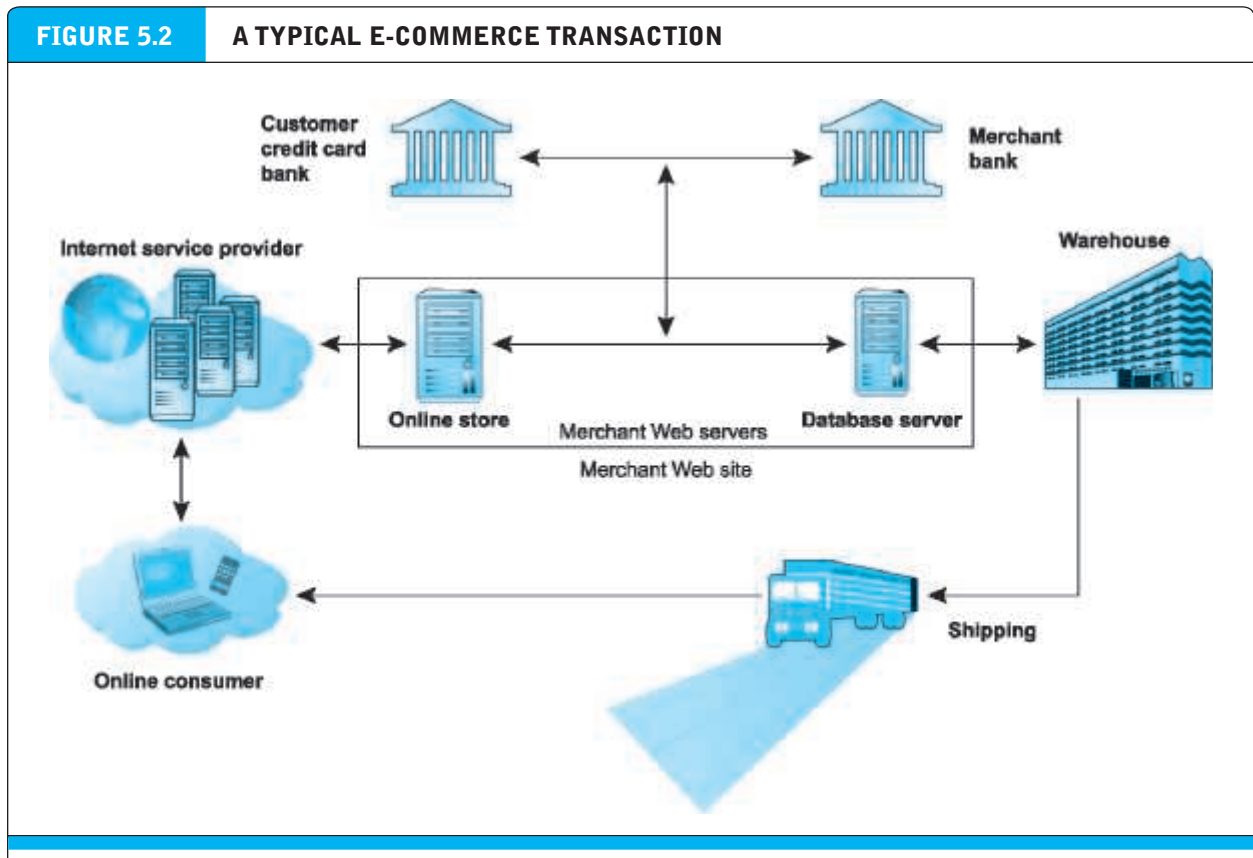
5.2 SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT

ضعف السهف

Name the major points of vulnerability in a typical online transaction?

From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the client, the server, and the communications pipeline.

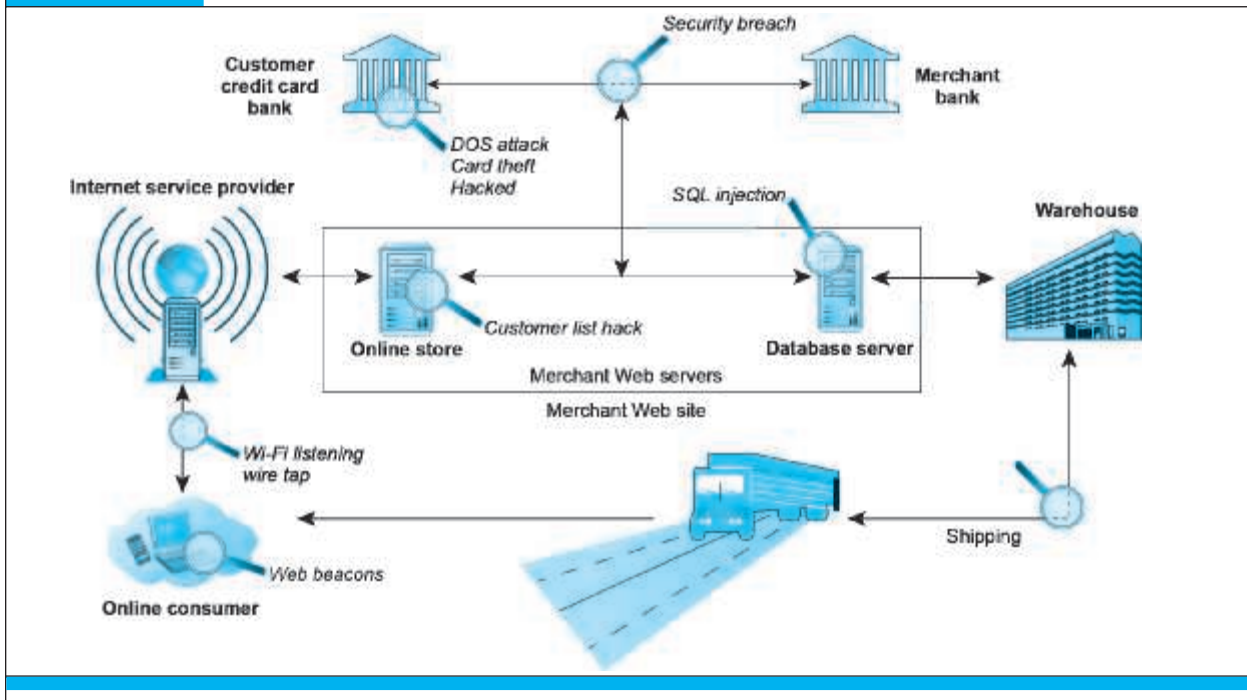
Figure 5.2 illustrates a typical e-commerce transaction with a consumer using a credit



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.

The key security threats in the e-commerce environment

MALICIOUS CODE

1

البرمجيات الضارة او الخبيثة

Malicious code is a threat to system's integrity and continued operations.

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.

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.

maladvertising

online advertising that contains malicious code

drive-by download

malware that comes with a downloaded file that a user requests

virus

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

kind

What are the influences of a virus on a computer?

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.

الغديه

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).

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

worm

malware that is designed to spread from computer to computer

ransomware (scareware)

malware that prevents you from accessing your computer or files and demands that you pay a fine

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

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

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.

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

in secrecy

غيبويه

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) 2

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 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, 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 3

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, 2004, tricky).

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

potentially unwanted program (PUP)

program that installs itself on a computer, typically without the user's informed consent agreement

why is adware or spyware considered to be a security threat?

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

spyware

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

social engineering

exploitation of human fallibility and gullibility to distribute malware

phishing

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

fraud

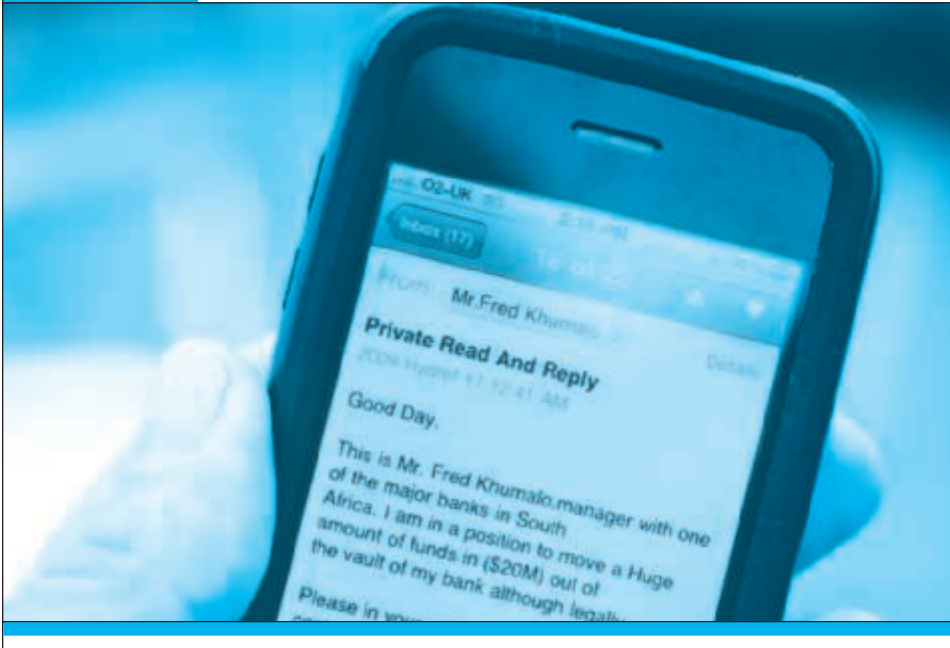
جشع

سداجه

cheat

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 “spoo”) 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 fail 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

4

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

cyber vandalism

intentionally disrupting, defacing, or even destroying a site

hacktivism

cyber vandalism 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 (**cyber vandalism**) 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 cyber vandalism, 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.

تشويه

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.

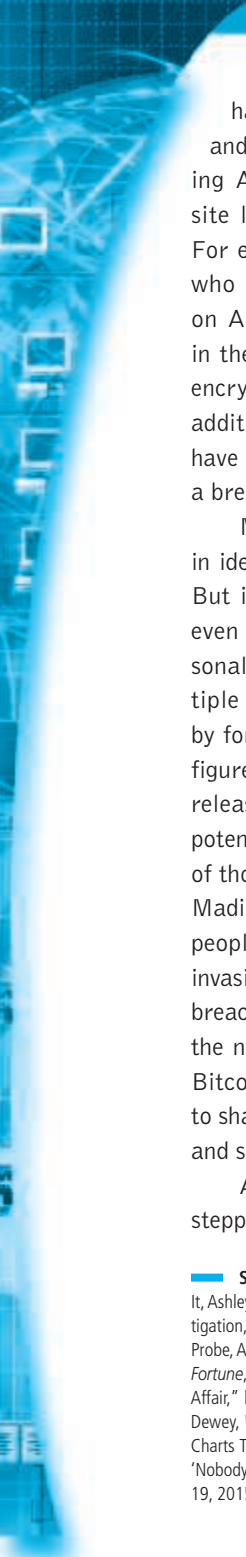
The perception of secrecy is critical for prospective users of Ashley Madison. But in 2015, that veil of secrecy came crashing down. The site was hacked by a group known as The Impact Team, which stated that its motivations were to harm the site and its unethical business model, as well as to protest 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).

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.

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.

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).

white hats

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

black hats

hackers who act with the intention of causing harm

grey hats

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

data breach

occurs when an organization loses control over its information to outsiders

CREDIT CARD FRAUD/THEFT 5

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

تزویر

6

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 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

7

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.

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-

make it too much

identity fraud

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

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

how does spoofing threaten a website's operators?

spoofing can threaten both the integrity and authenticity of a site, explain that?

deny

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.

تقنيات في المخزون

distinguish

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-redirectation domains such as topsearch10.com.

SNIFFING AND MAN-IN-THE-MIDDLE ATTACKS

8

التصنيت

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

9

Flood

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

what are the influence of DoS attack on a website?

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

المراقبة السلبية

1

2

unlimited

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 browsers 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

10

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 files, using risky applications, or accidentally downloading malware or clicking phishing links (Korolov, 2015).

POORLY DESIGNED SOFTWARE

11

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.

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.

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

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

zero-day vulnerability

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

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 12

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 1 in 2015 were manual sharing scams, where victims unwittingly shared videos, stories, 2 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 13

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

Some of the techniques
(types of scam) on
social media sites?

Rewards

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 apps, 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.

what are the influence of malicious mobile apps (Bluetooth worm) on mobile phone?

Some of the techniques or types of mobile cell malicious?

محتال

1

2

ساذج

التصيد الصوتي

هجوم الرسائل القصيرة

مستخدم برئ

INSIGHT ON TECHNOLOGY

THINK YOUR SMARTPHONE IS SECURE?

So far, there have been few publicly identified, large-scale, smartphone security breaches, but just because it hasn't happened yet doesn't mean it won't. With about 210 million smartphone users in the United States, business firms increasingly switching their employees to the mobile platform, and consumers using their phones for financial transactions and paying bills, the size and richness of the smartphone target for hackers is growing.

Many users believe their smartphones are unlikely to be hacked because Apple and Google are protecting them from malware, and that Verizon and AT&T can keep the cell phone network secure just as they do the land-line phone system. Telephone systems are "closed" and therefore not subject to the kinds of attacks that occur on the open Internet.

But hackers can do to a smartphone just about anything they can do to any Internet device: request malicious files without user intervention, delete files, transmit files, install programs running in the background that can monitor user actions, and potentially convert the smartphone into a robot that can be used in a botnet to send e-mail and text messages to anyone.

Apps are an emerging avenue for potential security breaches. Apple and Google now offer over 5 million apps collectively. Apple claims that it examines each and every app to ensure that it plays by Apple's App Store rules, but risks remain. In 2014, malware known as WireLurker attacked iPhone and iPad users in China via the Mac OS X operating system, representing the first attack on iPhones that were not jailbroken. Apple quickly moved to remove affected apps, but the attack was a warning sign that the iOS system is not likely to be a malware-

free environment going forward. In March 2016, new malware called AceDeceiver that infected non-jailbroken Apple devices circulated widely, scanning the App Store for other corrupted apps and automatically downloading them. That these corrupted apps were initially accepted by the App Store staff of reviewers suggests Apple cannot effectively review new apps prior to their use. This problem was further highlighted by a barrage of fake retail and product apps, primarily from developers in China, that also apparently slipped through Apple's review process and began appearing in the App Store preceding the 2016 holiday shopping season. Updates to the iOS operating system in 2016 exposed a series of vulnerabilities, collectively known as Trident, which allow attackers to take complete control of a phone remotely, without any indication that something has gone awry. Though Apple quickly scrambled to fix the vulnerability, releasing an operating system update in ten days, Trident showed that the iOS operating system is not as impervious to malware as many users believe. Any problems Apple has, it will have to fix by itself: third parties are not able to develop services to protect Apple devices as easily as they may be able to with Android because of Apple's "walled garden" approach. Overall, more malware affected iOS devices in 2015 than in the previous five years combined.

Android's security future appears just as murky. The amount of malware on the Android platform has skyrocketed over the past few years, with the number of spyware apps more than quadrupling from just a few years ago and doubling from 2015 to 2016. According to the Pulse Secure Mobile Threat Center, 97% of all mobile malware in 2015 targeted Android devices, and according to Nokia, more than 9 million Android

apps are vulnerable to remote attacks. In part this is due to the fact that security on the Android platform is much less under the control of Google because it employs an “open” app model compared to Apple’s, which makes security flaws easier to detect. In 2016, security firm Check Point reported that malware known as Hummingbad, which installs fraudulent apps and generates unwanted advertising, has infected approximately 10 million Android devices.

Android apps can use any personal information found on a phone but they must also inform the user what each app is capable of doing, and what personal data it requires. Google uses a universal scanning system that checks apps for malicious code and removes any apps that break its rules against malicious activity. Google can also perform a remote wipe of offending apps from all Droid phones without user intervention. In one incident, Google pulled down dozens of mobile banking apps made by a developer called 09Droid. The apps claimed to give users access to their accounts at many banks throughout the world. In fact, the apps were unable to connect users to any bank, and were removed before they could do much harm. Google does take preventive steps to reduce malware apps such as requiring developers to register and be approved by Google before they can distribute apps through Google Play.

Beyond the threat of rogue apps, smartphones of all stripes are susceptible to browser-

based malware that takes advantage of vulnerabilities in all browsers. In addition, most smartphones, including the iPhone, permit the manufacturers to remotely download configuration files to update operating systems and security protections. Unfortunately, flaws in the public key encryption procedures that permit remote server access to iPhones have been discovered, raising further questions about the security of such operations. Attackers have also developed methods of hijacking phones using weaknesses in SIM cards. There are at least 500 million vulnerable SIM cards in use today, and the defects allow hackers to obtain the encryption key that guards users’ personal information, granting them nearly complete access over the phone in the process. Many users don’t even take advantage of the security features they have available to them, such as the use of a lock screen, which only one-third of Android users have enabled.

In 2015, documents obtained by Edward Snowden indicated that the United States and Great Britain had hacked into Gemalto, a manufacturer of SIM cards, and obtained encryption keys that allowed them to surveil mobile phone users across the globe. The investigation is still ongoing, but after these revelations and a turbulent year of security breaches on both iOS and Android, our smartphones and tablets don’t seem quite as safe anymore.

SOURCES: “Beware, iPhone Users: Fake Retail Apps Are Surging Before Holidays,” by Vindu Goel, *New York Times*, November 6, 2016; “Microsoft: ‘Apple Can No More Secure Your iPhone Than Google Can Secure Android,’” by Zdnet.com, October 14, 2016; “Top 10 Ways to Secure Your Mobile Phone,” by Wendy Zamora, *Blog.malwarebytes.com*, September 21, 2016; “Smartphone Infections Double, Hotspots Are Also a Trouble Area,” by Patrick Nelson, *Networkworld.com*, September 7, 2016; “iPhone Malware That Steals Your Data Proves No Platform is Truly Secure,” by Liam Tung and Raymond Wong, *Mashable.com*, August 26, 2016; “This App Can Tell If an iPhone Was Hacked With Latest Pegasus Spy Malware,” by Janko Roettgers, *Variety.com*, August 26, 2016; “iPhone Users Urged to Update Software After Security Flaws Are Found,” by Nicole Perloth, *New York Times*, August 25, 2016; “Hummingbad Malware Infects 10 Million Devices: How to Check If Your Phone or Tablet Is Among Them,” by Aaron Mamiit, *Techtimes.com*, July 6, 2016; “This Nasty New Malware Can Infect Your Apple iPhone or iPad,” by Jonathan Vanian, *Fortune*, March 16, 2016; “Mobile Malware on Smartphones and Tablets: The Inconvenient Truth,” by Shaked Vax, *Securityintelligence.com*, February 15, 2016; “Android Accounts for 97 Percent of All Mobile Malware,” by Carly Page, *Theinquirer.net*, June 25, 2015; “Digital-Security Firm Gemalto Probes Alleged U.S., U.K. Hack,” by Amir Mizroch and Lisa Fleisher, *Wall Street Journal*, February 20, 2015; “US and UK Accused of Hacking SIM Card Firm to Steal Codes,” *Bbc.com*, February 20, 2015; “XAgent iPhone Malware Attack Steals Data Without Jailbreaking,” by Jeff Gamet, *Macobserver.com*, February 5, 2015; “Apple Blocks Apps Infected with WireLurker Malware Targeting iPhones and iPads,” by Carly Page, *Theinquirer.net*, November 6, 2014; “NSA Secretly Broke Smartphone Security,” by Cory Doctorow, *Boingboing.com*, September 8, 2013; “Obama Administration Had Restrictions on NSA Reversed in 2011,” by Ellen Nakashima, September 7, 2013; “How Google Just Quietly Made Your Android Phone More Secure,” by JR Raphael, *Computerworld*, July 26, 2013.

CLOUD SECURITY ISSUES

14

The move of so many Internet services into the cloud also raises security risks. From an infrastructure standpoint, DDoS attacks threaten the availability of cloud services on which more and more companies are relying. For instance, as previously noted, the DDoS attack on Dyn in 2016 caused a major disruption to cloud services across the United States. According to Alert Logic, which analyzed 1 billion security events in the IT environments of more than 3,000 enterprise customers, attacks against cloud-based services and applications increased by 45%. Alert Logic also found a 36% increase in suspicious activity in cloud environment, such as attempts to scan the infrastructure (Alert Logic, 2015). Safeguarding data being maintained in a public cloud environment is also a major concern (Cloud Security Alliance, 2016). For example, researchers identified several ways data could be accessed without authorization on Dropbox, which offers a popular cloud file-sharing service. In 2014, compromising photos of as many as 100 celebrities such as Jennifer Lawrence were posted online, reportedly stolen from Apple's iCloud. Although initially it was thought that the breach was made possible by a vulnerability in Apple's Find My iPhone API, it instead apparently resulted from lower-tech phishing attacks that yielded passwords that could be used to connect to iCloud. A similar hack into writer Mat Honan's Apple iCloud account using social engineering tactics in 2012 allowed the hackers to wipe everything from his Mac computer, iPhone, and iPad, which were linked to the cloud service, as well as take over his Twitter and Gmail accounts (Honan, 2012). These incidents highlight the risks involved as devices, identities, and data become more and more interconnected in the cloud. A 2016 Ponemon Institute study of 3,400 IT executives found that the majority of IT and IT security practitioners surveyed felt that the likelihood of a data breach increases due to the cloud, in part due to the fact that many organizations do not thoroughly examine cloud security before deploying cloud services. The study also found that only one-third of sensitive data in cloud-based applications was encrypted, and that half of the firms involved do not have a proactive approach to cloud security, relying instead on the cloud providers to ensure security (Loten, 2016; Gemalto and Ponemon, 2016).

INTERNET OF THINGS SECURITY ISSUES

15

As you learned in Chapter 3, the Internet of Things (IoT) involves the use of the Internet to connect a wide variety of sensors, devices, and machines, and is powering the development of a multitude of smart connected things, such as home electronics (smart TVs, thermostats, home security systems, and more), connected cars, medical devices, and industrial equipment that supports manufacturing, energy, transportation, and other industrial sectors. IoT raises a host of security issues that are in some ways similar to existing security issues, but even more challenging, given the need to deal with a wider range of devices, operating in a less controlled, global environment, and with an expanded range of attack. In a world of connected things, the devices, the data produced and used by the devices, and the systems and applications supported by those devices, can all potentially be attacked (IBM, 2015). Table 5.5 takes a closer look at some of the unique security challenges posed by IoT identified

The vulnerabilities in the Internet of things?

3

2

1

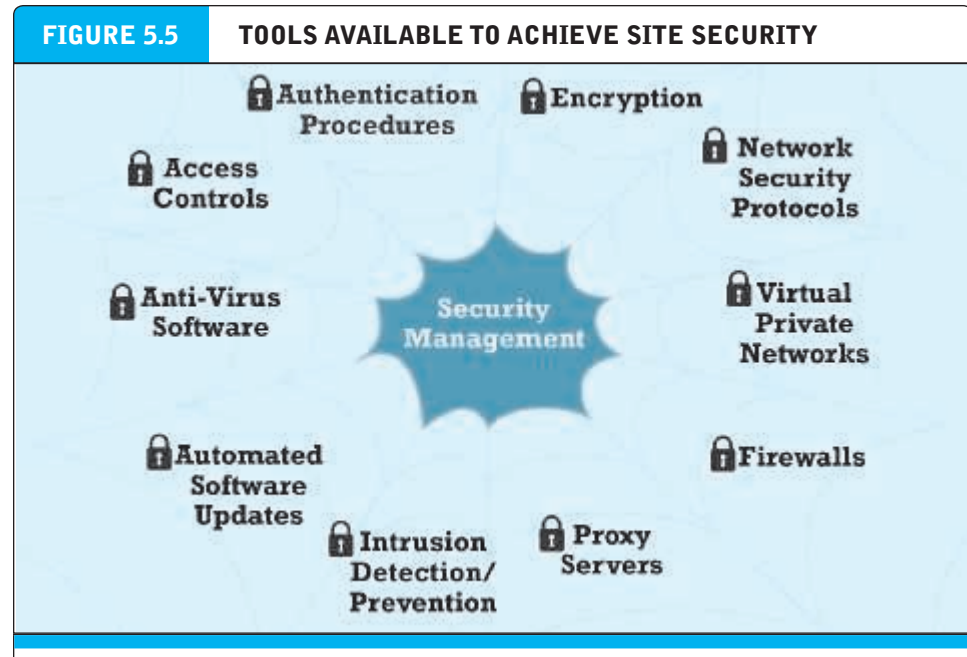
TABLE 5.5

INTERNET OF THINGS SECURITY CHALLENGES

CHALLENGE	POSSIBLE IMPLICATIONS
1 Many IoT devices, such as sensors, are intended to be deployed on a much greater scale than traditional Internet-connected devices, creating a vast quantity of interconnected links that can be exploited.	Existing tools, methods, and strategies need to be developed to deal with this <u>unprecedented scale</u> . غير مسبوق
2 Many instances of IoT consist of collections of identical devices that all have the same characteristics.	Magnifies the potential impact of a security vulnerability.
3 Many IoT devices are <u>anticipated</u> to have a much longer service life than typical equipment.	Devices may “outlive” manufacturer, leaving them without long-term support that creates <u>persistent vulnerabilities</u> . continuous
4 Many IoT devices are intentionally designed without the ability to be upgraded, or the upgrade process is difficult.	Raises the possibility that vulnerable devices cannot or will not be fixed, leaving them perpetually vulnerable.
5 Many IoT devices do not provide the user with visibility into the workings of the device or the data being produced, nor alert the user when a security problem arises.	Users may believe an IoT device is functioning as intended when in fact, it may be performing in a malicious manner.
6 Some IoT devices, such as sensors, are unobtrusively embedded in the environment such that a user may not even be aware of the device.	Security breach might persist for a long time before being noticed.

by the [Internet Society \(ISOC\)](#), a consortium of corporations, government agencies, and nonprofit organizations that monitors Internet policies and practices (Internet Society, 2016, 2015).

Already, alarming reports of hacked IoT devices are starting to pop up in the popular press. For example, in July 2015, researchers demonstrated the ability to hack into a Jeep Cherokee through its entertainment system, sending commands to the dashboard, steering, brakes, and transmission system from a remote laptop that turned the steering wheel, disabled the brakes, and shut down the engine (Greenberg, 2015). Fiat Chrysler Automobiles immediately issued a recall notice to fix the software vulnerability involved, but it is almost certain that such incidents will continue to occur, as auto manufacturers add more and more wireless “connected car” features to automobiles. Other reports have surfaced of wireless baby monitors being hacked, as well as medical devices such as hospital lab blood gas analyzers, radiology picture archive and communication systems, drug infusion pumps, and hospital x-ray systems (Storm, 2015a, 2015b). The previously mentioned DDoS 2016 attack on Dyn relied in part on millions of Internet-connected security cameras (Sanger and Perlroth, 2016).



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

5.3 TECHNOLOGY SOLUTIONS

Attack

destructive

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 1

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.”

1 **Symmetric Key Cryptography**

There are a variety of different forms of encryption technology currently in use. They include:

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,

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 (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.

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 2

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.

Data Encryption

Standard (DES)

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

Advanced Encryption

Standard (AES)

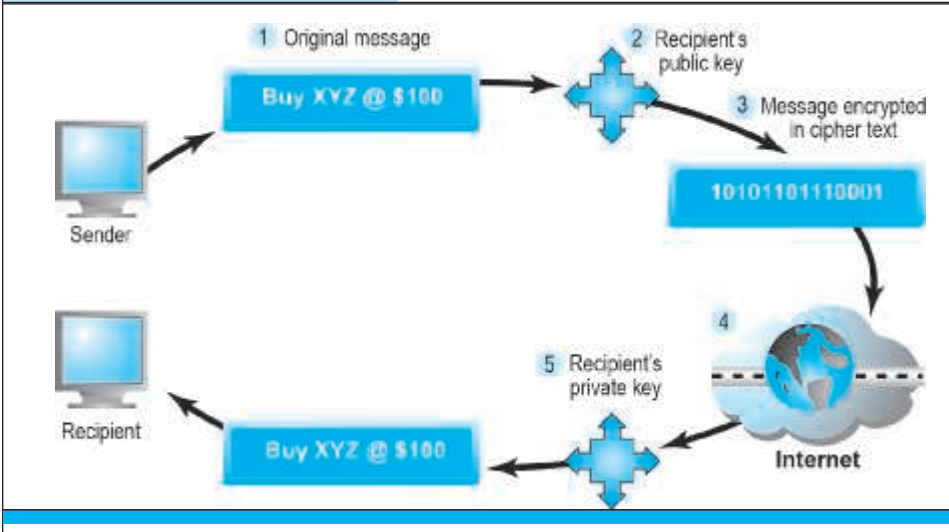
the most widely used symmetric key algorithm, offering 128-, 192-, and 256-bit keys

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

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

3

It guarantee the message confidentiality but

- no authentication of the sender (repudiation)

- Integrity

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.

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.

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

hash function

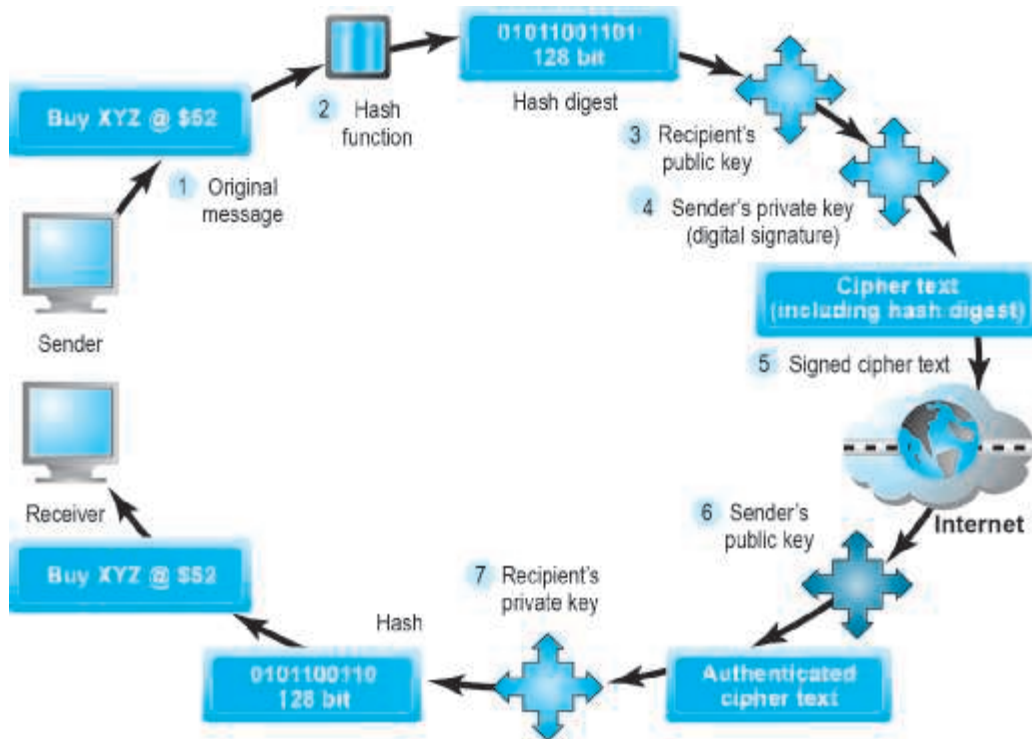
an algorithm that produces a fixed-length number called a hash or message digest

digital signature (e-signature)

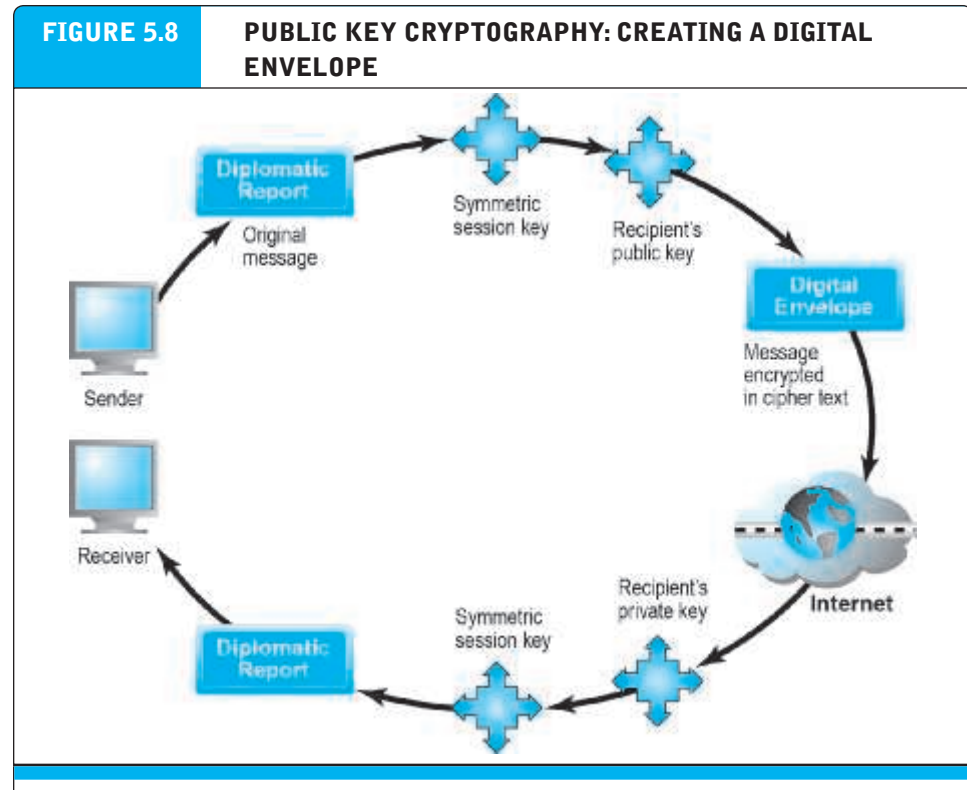
“signed” cipher text that can be sent over the Internet

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.



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.

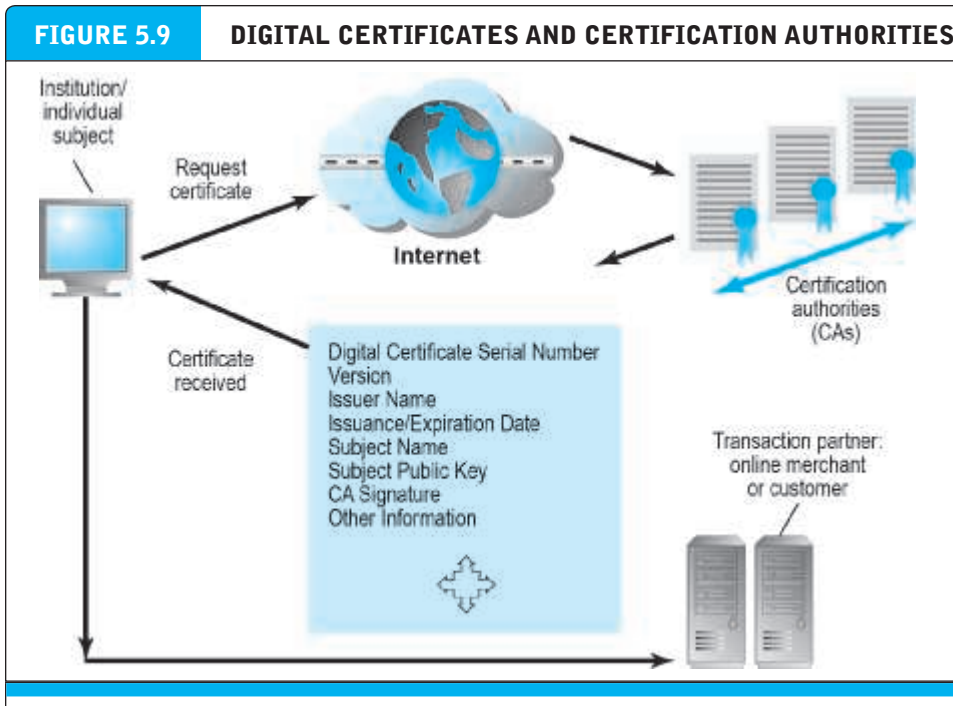
Digital Envelopes

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.

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

digital envelope

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



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.

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.

**Pretty Good Privacy
(PGP)**

a widely used e-mail public key encryption software program

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

do not store customer information in encrypted form. Other limitations are apparent. For one, how is your private key to be protected? Most private keys will be stored on insecure desktop or laptop computers.

There is no guarantee the person using your computer—and your private key—is really you. For instance, you may lose your laptop or smartphone, and therefore lose the private key. Likewise, there is no assurance that someone else in the world cannot use your personal ID papers, such as a social security card, to obtain a PKI authenticated online ID in your name. If there's no real world identification system, there can be no truly secure Internet identification system. Under many digital signature laws, you are responsible for whatever your private key does even if you were not the person using the key. This is very different from mail-order or telephone order credit card rules, where you have a right to dispute the credit card charge. Second, there is no guarantee the verifying computer of the merchant is secure. Third, CAs are self-selected organizations seeking to gain access to the business of authorization. They may not be authorities on the corporations or individuals they certify. For instance, how can a CA know about all the corporations within an industry to determine who is or is not legitimate? A related question concerns the method used by the CA to identify the certificate holder. Was this an e-mail transaction verified only by claims of the applicants who filled out an online form? For instance, VeriSign acknowledged in one case that it had mistakenly issued two digital certificates to someone fraudulently claiming to represent Microsoft. Digital certificates have been hijacked by hackers, tricking consumers into giving up personal information. For example, in 2014, India's National Informatics Centre, an intermediate CA that was trusted by the Indian Controller of Certifying Authorities, whose certificates were included in the Microsoft Root Store and thus trusted by the vast majority of programs running on Windows, including Internet Explorer and Chrome, was hacked and a number of unauthorized digital certificates were issued for domains operated by Google and Yahoo (Datta, 2014). Last, what are the policies for revoking or renewing certificates? The expected life of a digital certificate or private key is a function of the frequency of use and the vulnerability of systems that use the certificate. Yet most CAs have no policy or just an annual policy for reissuing certificates. If Microsoft, Apple, or Cisco ever rescinded a number of CAs, millions of users would not be able to access sites. The CA system is difficult and costly to police.

SECURING CHANNELS OF COMMUNICATION

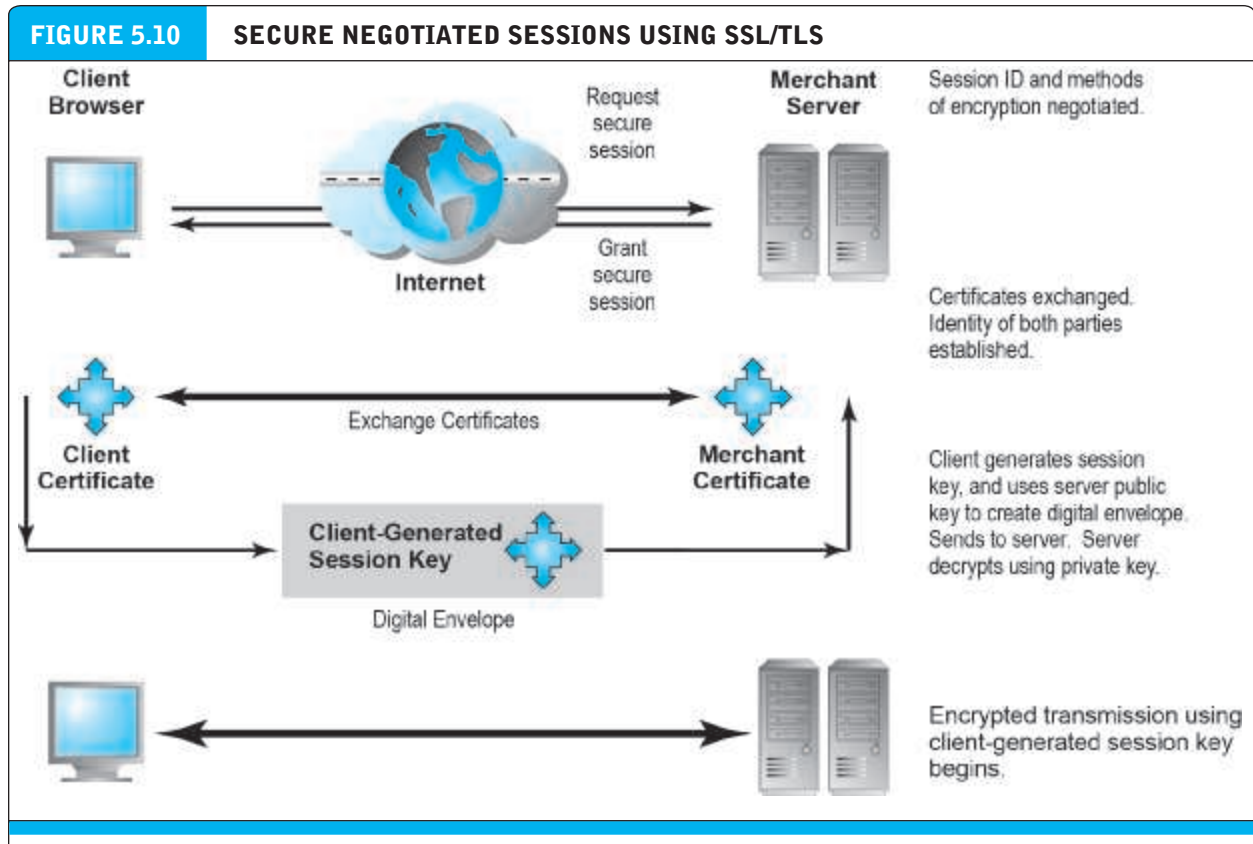
The concepts of public key cryptography are used routinely for securing channels of communication.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

The most common form of securing channels is through the *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS)* protocols. When you receive a message from a server on the Web with which you will be communicating through a secure channel, this means you will be using SSL/TLS to establish a secure negotiated session. (Notice that the URL changes from HTTP to HTTPS.) A **secure negotiated session** is a client-

secure negotiated session

a client-server session in which the URL of the requested document, along with the contents, contents of forms, and the cookies exchanged, are encrypted



Certificates play a key role in using SSL/TLS to establish a secure communications channel.

server session in which the URL of the requested document, along with the contents, contents of forms, and the cookies exchanged, are encrypted (see **Figure 5.10**). For instance, your credit card number that you entered into a form would be encrypted. Through a series of handshakes and communications, the browser and the server establish one another's identity by exchanging digital certificates, decide on the strongest shared form of encryption, and then proceed to communicate using an agreed-upon session key. A **session key** is a unique symmetric encryption key chosen just for this single secure session. Once used, it is gone forever. Figure 5.10 shows how this works.

session key

a unique symmetric encryption key chosen for a single secure session

In practice, most private individuals do not have a digital certificate. In this case, the merchant server will not request a certificate, but the client browser will request the merchant certificate once a secure session is called for by the server.

SSL/TLS provides data encryption, server authentication, optional client authentication, and message integrity for TCP/IP connections. SSL/TLS addresses the issue of authenticity by allowing users to verify another user's identity or the identity of a server. It also protects the integrity of the messages exchanged. However, once the merchant receives the encrypted credit and order information, that information is typi-

cally stored in unencrypted format on the merchant's servers. While SSL/TLS provides secure transactions between merchant and consumer, it only guarantees server-side authentication. Client authentication is optional.

In addition, SSL/TLS cannot provide irrefutability—consumers can order goods or download information products, and then claim the transaction never occurred. Recently, social network sites such as Facebook and Twitter have begun to use SSL/TLS for a variety of reasons, including the ability to thwart account hijacking using Firesheep over wireless networks. Firesheep, an add-on for Firefox, can be used by hackers to grab unencrypted cookies used to “remember” a user and allow the hacker to immediately log on to a website as that user. SSL/TLS can thwart such an attack because it encrypts the cookie. In June 2015, the White House's Office of Management and Budget issued a memorandum requiring that all publicly accessible federal websites and web services use HTTPS by December 31, 2016. HTTPS encrypts user requests to website servers. It is implemented by the server adopting the HTTP Strict Transport Security (HSTS) feature that forces browsers to only access the server using HTTPS (CIO.gov, 2016).

Virtual Private Networks (VPNs)

2

A virtual private network (VPN) allows remote users to securely access a corporation's local area network via the Internet, using a variety of VPN protocols. VPNs use both authentication and encryption to secure information from unauthorized persons (providing confidentiality and integrity). Authentication prevents spoofing and misrepresentation of identities. A remote user can connect to a remote private local network using a local ISP. The VPN protocols will establish the link from the client to the corporate network as if the user had dialed into the corporate network directly. The process of connecting one protocol through another (IP) is called *tunneling*, because the VPN creates a private connection by adding an invisible wrapper around a message to hide its content. As the message travels through the Internet between the ISP and the corporate network, it is shielded from prying eyes by an encrypted wrapper.

A VPN is “virtual” in the sense that it appears to users as a dedicated secure line when in fact it is a temporary secure line. The primary use of VPNs is to establish secure communications among business partners—larger suppliers or customers, and employees working remotely. A dedicated connection to a business partner can be very expensive. Using the Internet and VPN as the connection method significantly reduces the cost of secure communications.

Wireless (Wi-Fi) Networks

Accessing the Internet via a wireless (Wi-Fi) network has its own particular security issues. Early Wi-Fi networks used a security standard called Wired Equivalent Privacy (WEP) to encrypt information. WEP was very weak, and easy for hackers to crack. A new standard, Wi-Fi Protected Access (WPA), was developed that provided a higher standard of protection, but this too soon became vulnerable to intrusion. Today, the current standard is **WPA2**, which uses the AES algorithm for encryption and CCMP, a more advanced authentication code protocol.

virtual private network (VPN)

allows remote users to securely access internal networks via the Internet, using the Point-to-Point Tunneling Protocol (PPTP)

WPA2

wireless security standard that uses the AES algorithm for encryption and CCMP, a more advanced authentication code protocol

PROTECTING NETWORKS

Once you have protected communications as well as possible, the next set of tools to consider are those that can protect your networks, as well as the servers and clients on those networks.

Firewalls

3

Firewalls and proxy servers are intended to build a wall around your network and the attached servers and clients, just like physical-world firewalls protect you from fires for a limited period of time. Firewalls and proxy servers share some similar functions, but they are quite different.

firewall

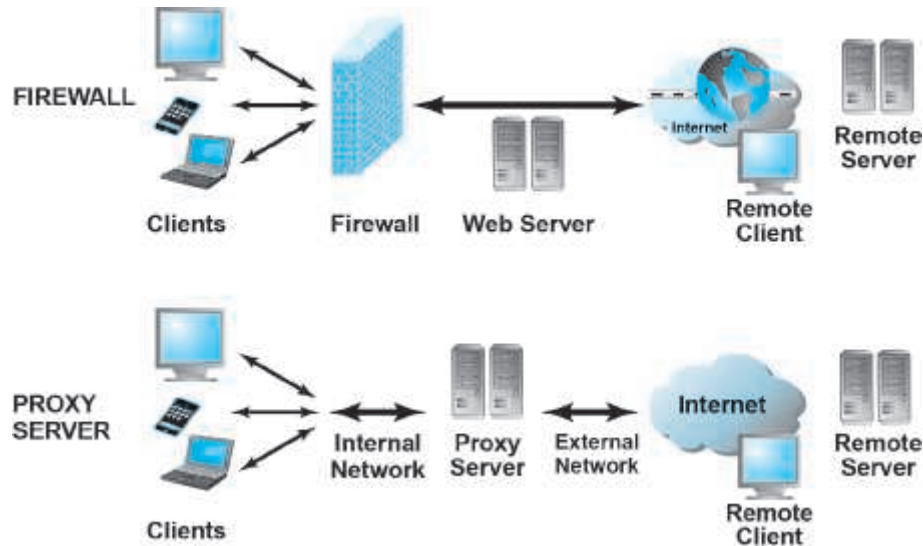
refers to either hardware or software that filters communication packets and prevents some packets from entering the network based on a security policy

A firewall refers to either **hardware or software that filters communication packets and prevents some packets from entering or exiting the network based on a security policy**. The firewall controls traffic to and from servers and clients, forbidding communications from untrustworthy sources, and allowing other communications from trusted sources to proceed. Every message that is to be sent or received from the network is processed by the firewall, which determines if the message meets security guidelines established by the business. If it does, it is permitted to be distributed, and if it doesn't, the message is blocked. **Firewalls can filter traffic based on packet attributes such as source IP address, destination port or IP address, type of service (such as WWW or HTTP), the domain name of the source, and many other dimensions**. Most hardware firewalls that protect local area networks connected to the Internet have default settings that require little if any administrator intervention and employ simple but effective rules that deny incoming packets from a connection that does not originate from an internal request—the firewall only allows connections from servers that you requested service from. A common default setting on hardware firewalls (DSL and cable modem routers) simply ignores efforts to communicate with TCP port 445, the most commonly attacked port. The increasing use of firewalls by home and business Internet users has greatly reduced the effectiveness of attacks, and forced hackers to focus more on e-mail attachments to distribute worms and viruses.

There are two major methods firewalls use to validate traffic: packet filters and application gateways. *Packet filters* examine data packets to determine whether they are destined for a prohibited port or originate from a prohibited IP address (as specified by the security administrator). The filter specifically looks at the source and destination information, as well as the port and packet type, when determining whether the information may be transmitted. One downside of the packet filtering method is that it is susceptible to spoofing, because authentication is not one of its roles.

Application gateways are a type of firewall that filters communications based on the application being requested, rather than the source or destination of the message. Such firewalls also process requests at the application level, farther away from the client computer than packet filters. By providing a central filtering point, application gateways provide greater security than packet filters but can compromise system performance.

Next-generation firewalls use an application-centric approach to firewall control. They are able to identify applications regardless of the port, protocol, or security evasion tools used; identify users regardless of device or IP address; decrypt outbound SSL; and protect in real-time against threats embedded in applications.

FIGURE 5.11 FIREWALLS AND PROXY SERVERS

The primary function of a firewall is to deny access by remote client computers to local computers. The primary purpose of a proxy server is to provide controlled access from local computers to remote computers.

Proxy Servers

4

Proxy servers (proxies) are software servers (often a dedicated computer) that handle all communications originating from or being sent to the Internet by local clients, acting as a spokesperson or bodyguard for the organization. Proxies act primarily to limit access of internal clients to external Internet servers, although some proxy servers act as firewalls as well. Proxy servers are sometimes called *dual-home systems* because they have two network interfaces. To internal computers, a proxy server is known as the *gateway*, while to external computers it is known as a *mail server* or *numeric address*.

When a user on an internal network requests a web page, the request is routed first to the proxy server. The proxy server validates the user and the nature of the request, and then sends the request onto the Internet. A web page sent by an external Internet server first passes to the proxy server. If acceptable, the web page passes onto the internal network web server and then to the client desktop. By prohibiting users from communicating directly with the Internet, companies can restrict access to certain types of sites, such as pornographic, auction, or stock-trading sites. Proxy servers also improve web performance by storing frequently requested web pages locally, reducing upload times, and hiding the internal network's address, thus making it more difficult for hackers to monitor. **Figure 5.11** illustrates how firewalls and proxy servers protect a local area network from Internet intruders and prevent internal clients from reaching prohibited web servers.

proxy server (proxy)

software server that handles all communications originating from or being sent to the Internet, acting as a spokesperson or bodyguard for the organization

التسلسل

intrusion detection system (IDS)

examines network traffic, watching to see if it matches certain patterns or preconfigured rules indicative of an attack

intrusion prevention system (IPS)

has all the functionality of an IDS, with the additional ability to take steps to prevent and block suspicious activities

Intrusion Detection and Prevention Systems

5

In addition to a firewall and proxy server, an intrusion detection and/or prevention system can be installed. **An intrusion detection system (IDS) examines network traffic, watching to see if it matches certain patterns or preconfigured rules indicative of an attack. If it detects suspicious activity, the IDS will set off an alarm alerting administrators and log the event in a database.** An IDS is useful for detecting malicious activity that a firewall might miss. **An intrusion prevention system (IPS) has all the functionality of an IDS, with the additional ability to take steps to prevent and block suspicious activities.** For instance, an IPS can terminate a session and reset a connection, block traffic from a suspicious IP address, or reconfigure firewall or router security controls.

PROTECTING SERVERS AND CLIENTS

Operating system features and anti-virus software can help further protect servers and clients from certain types of attacks.

Operating System Security Enhancements

6

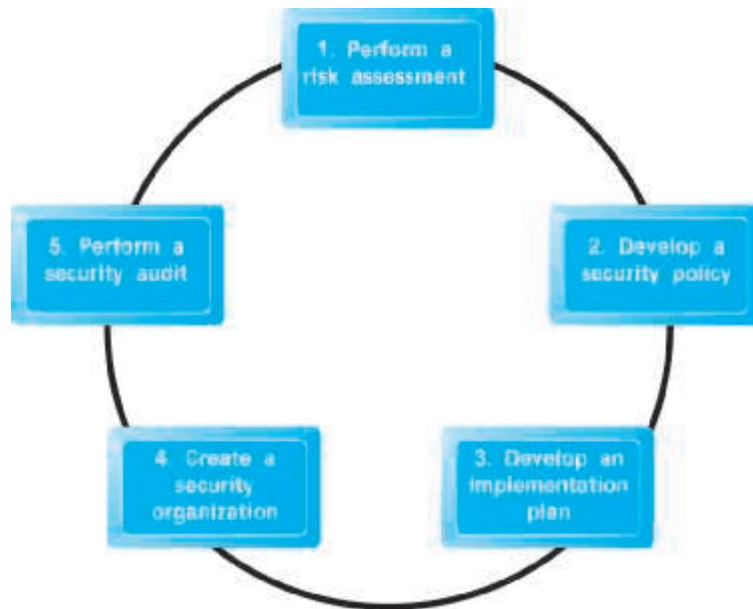
The most obvious way to protect servers and clients is to take advantage of automatic computer security upgrades. The Microsoft, Apple, and Linux/Unix operating systems are continuously updated to patch vulnerabilities discovered by hackers. These patches are autonomic; that is, when using these operating systems on the Internet, you are prompted and informed that operating system enhancements are available. Users can easily download these security patches for free. The most common known worms and viruses can be prevented by simply keeping your server and client operating systems and applications up to date. In April 2014, Microsoft ended security support and updates for its Windows XP operating system. Despite this, many organizations continue to use XP-based systems, and as a result, many security experts anticipate a wave of strikes against such systems. Application vulnerabilities are fixed in the same manner. For instance, most popular Internet browsers are updated automatically with little user intervention.

Anti-Virus Software

7

The easiest and least-expensive way to prevent threats to system integrity is to install anti-virus software. Programs by Malwarebytes, McAfee, Symantec (Norton AntiVirus), and many others provide inexpensive tools to identify and eradicate the most common types of malicious code as they enter a computer, as well as destroy those already lurking on a hard drive. Anti-virus programs can be set up so that e-mail attachments are inspected before you click on them, and the attachments are eliminated if they contain a known virus or worm. It is not enough, however, to simply install the software once. Because new viruses are developed and released every day, daily routine updates are needed in order to prevent new threats from being loaded. Some premium-level anti-virus software is updated hourly.

Anti-virus suite packages and stand-alone programs are available to eliminate intruders such as bot programs, adware, and other security risks. Such programs work much like anti-virus software in that they look for recognized hacker tools or signature actions of known intruders.

FIGURE 5.12 DEVELOPING AN E-COMMERCE SECURITY PLAN

There are five steps involved in building an e-commerce security plan.

5.4 MANAGEMENT POLICIES, BUSINESS PROCEDURES, AND PUBLIC LAWS

Worldwide, in 2016, companies are expected to spend over \$81 billion on security hardware, software, and services, up 8% from the previous year (Gartner, 2016). However, most CEOs and CIOs believe that technology is not the sole answer to managing the risk of e-commerce. The technology provides a foundation, but in the absence of intelligent management policies, even the best technology can be easily defeated. Public laws and active enforcement of cybercrime statutes also are required to both raise the costs of illegal behavior on the Internet and guard against corporate abuse of information. Let's consider briefly the development of management policy.

A SECURITY PLAN: MANAGEMENT POLICIES

In order to minimize security threats, e-commerce firms must develop a coherent corporate policy that takes into account the nature of the risks, the information assets that need protecting, and the procedures and technologies required to address the risk, as well as implementation and auditing mechanisms. **Figure 5.12** illustrates the key steps in developing a solid security plan.

1

risk assessment

an assessment of the risks and points of vulnerability

A security plan begins with **risk assessment**—an assessment of the risks and points of vulnerability. The first step is to inventory the information and knowledge assets of the e-commerce site and company. What information is at risk? Is it customer information, proprietary designs, business activities, secret processes, or other internal information, such as price schedules, executive compensation, or payroll? For each type of information asset, try to estimate the dollar value to the firm if this information were compromised, and then multiply that amount by the probability of the loss occurring. Once you have done so, rank order the results. You now have a list of information assets prioritized by their value to the firm.

2

security policy

a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets

Based on your quantified list of risks, you can start to develop a **security policy**—a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets. You will obviously want to start with the information assets that you determined to be the highest priority in your risk assessment. Who generates and controls this information in the firm? What existing security policies are in place to protect the information? What enhancements can you recommend to improve security of these most valuable assets? What level of risk are you willing to accept for each of these assets? Are you willing, for instance, to lose customer credit card data once every 10 years? Or will you pursue a 100-year hurricane strategy by building a security edifice for credit card data that can withstand the once-in-100-year disaster? You will need to estimate how much it will cost to achieve this level of acceptable risk. Remember, total and complete security may require extraordinary financial resources. By answering these questions, you will have the beginnings of a security policy.

3

implementation plan

the action steps you will take to achieve the security plan goals

Next, consider an **implementation plan**—the steps you will take to achieve the security plan goals. Specifically, you must determine how you will translate the levels of acceptable risk into a set of tools, technologies, policies, and procedures. What new technologies will you deploy to achieve the goals, and what new employee procedures will be needed?

4

security organization

educates and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security

To implement your plan, you will need an organizational unit in charge of security, and a security officer—someone who is in charge of security on a daily basis. For a small e-commerce site, the security officer will likely be the person in charge of Internet services or the site manager, whereas for larger firms, there typically is a dedicated team with a supporting budget. The security organization educates and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security.

A

access controls

determine who can gain legitimate access to a network

The security organization typically administers access controls, authentication procedures, and authorization policies. Access controls determine which outsiders and insiders can gain legitimate access to your networks. Outsider access controls include firewalls and proxy servers, while insider access controls typically consist of login procedures (usernames, passwords, and access codes).

B

authentication procedures

include the use of digital signatures, certificates of authority, and public key infrastructure

المصادقة

Authentication procedures include the use of digital signatures, certificates of authority, and PKI. Now that e-signatures have been given the same legal weight as an original pen-and-ink version, companies are in the process of devising ways to test and confirm a signer's identity. Companies frequently have signers type their full

name and click on a button indicating their understanding that they have just signed a contract or document.

Biometric devices can also be used to verify physical attributes associated with an individual, such as a fingerprint or retina (eye) scan or speech recognition system. (**Biometrics** is the study of measurable biological, or physical, characteristics.) A company could require, for example, that an individual undergo a fingerprint scan before being allowed access to a website, or before being allowed to pay for merchandise with a credit card. Biometric devices make it even more difficult for hackers to break into sites or facilities, significantly reducing the opportunity for spoofing. Newer Apple iPhones (5S and later) feature a fingerprint sensor called Touch ID built into the iPhone's home button that can unlock the phone and authorize purchases from the iTunes, iBooks, and App Stores without requiring users to enter a PIN or other security code. According to Apple, the system does not store an actual fingerprint, but rather biometric data, which will be encrypted and stored only on a chip within the iPhone, and will not be made available to third parties.

Security tokens are physical devices or software that generate an identifier that can be used in addition to or in place of a password. Security tokens are used by millions of corporation and government workers to log on to corporate clients and servers. One example is RSA's SecurID token, which continuously generates six-digit passwords.

Authorization policies determine differing levels of access to information assets for differing levels of users. **Authorization management systems** establish where and when a user is permitted to access certain parts of a website. Their primary function is to restrict access to private information within a company's Internet infrastructure. Although there are several authorization management products currently available, most operate in the same way: the system encrypts a user session to function like a passkey that follows the user from page to page, allowing access only to those areas that the user is permitted to enter, based on information set at the system database. By establishing entry rules up front for each user, the authorization management system knows who is permitted to go where at all times.

The last step in developing an e-commerce security plan is performing a security audit. **A security audit** involves the routine review of access logs (identifying how outsiders are using the site as well as how insiders are accessing the site's assets). A monthly report should be produced that establishes the routine and nonroutine accesses to the systems and identifies unusual patterns of activities. As previously noted, tiger teams are often used by large corporate sites to evaluate the strength of existing security procedures. Many small firms have sprung up in the last five years to provide these services to large corporate sites.

THE ROLE OF LAWS AND PUBLIC POLICY

The public policy environment today is very different from the early days of e-commerce. The net result is that the Internet is no longer an ungoverned, unsupervised, self-controlled technology juggernaut. Just as with financial markets in the last 70 years, there is a growing awareness that e-commerce markets work only when a powerful institutional set of laws and enforcement mechanisms are in place. These laws

biometrics

the study of measurable biological or physical characteristics

security token

physical device or software that generates an identifier that can be used in addition to or in place of a password

authorization policies determine differing levels of access to information assets for differing levels of users

authorization management system

establishes where and when a user is permitted to access certain parts of a website

security audit

involves the routine review of access logs (identifying how outsiders are using the site as well as how insiders are accessing the site's assets)

C

5

help ensure orderly, rational, and fair markets. This growing public policy environment is becoming just as global as e-commerce itself. Despite some spectacular internationally based attacks on U.S. e-commerce sites, the sources and persons involved in major harmful attacks have almost always been uncovered and, where possible, prosecuted.

Voluntary and private efforts have played a very large role in identifying criminal hackers and assisting law enforcement. Since 1995, as e-commerce has grown in significance, national and local law enforcement activities have expanded greatly. New laws have been passed that grant local and national authorities new tools and mechanisms for identifying, tracing, and prosecuting cybercriminals. For instance, a majority of states now require companies that maintain personal data on their residents to publicly disclose when a security breach affecting those residents has occurred. **Table 5.6** lists the most significant federal e-commerce security legislation and regulation. In addition, the Federal Trade Commission has asserted that it has authority over corporations' data security practices. The FTC sued the Wyndham hotel chain after hacking attacks in 2008 and 2009 resulted in a data breach that led to fraudulent credit charges of more than \$10 million. According to the FTC, its investigation showed that Wyndham had failed to follow basic data security practices, while at the same time assuring customers that their data was safe. In August 2015, the U.S. Court of Appeals for the Third Circuit ruled that the FTC was within the scope of its authority, opening the door for it to take a greater role, especially in light of the failure of Congress to adopt legislation governing data security. By increasing the punishment for cybercrimes, the U.S. government is attempting to create a deterrent to further hacker actions. And by making such actions federal crimes, the government is able to extradite international hackers and prosecute them within the United States.

After September 11, 2001, Congress passed the USA PATRIOT Act, which broadly expanded law enforcement's investigative and surveillance powers. The act has provisions for monitoring e-mail and Internet use. The Homeland Security Act of 2002 also attempts to fight cyberterrorism and increases the government's ability to compel information disclosure by computer and ISP sources. Recent proposed legislation that focuses on requiring firms to report data breaches to the FTC, protection of the national electric grid, and cybersecurity has all failed to pass. However, in December 2015, the Cybersecurity Information Sharing Act (CISA) was signed into law by President Obama. The Act, which creates a system that lets companies share evidence about attacks without the risk of being sued, had been opposed by many large technology companies and privacy advocates on the grounds that it did not do enough to protect individual privacy and could lead to increased government surveillance. However, implementation of the CISA is still a work in progress and it remains to be seen how effective it will be (Chew and Newby, 2016; Peterson, 2015).

Private and Private-Public Cooperation Efforts

The good news is that e-commerce sites are not alone in their battle to achieve security on the Internet. Several organizations—some public and some private—are

TABLE 5.6

E-COMMERCE SECURITY LEGISLATION AND REGULATION

LEGISLATION/REGULATION	SIGNIFICANCE
Computer Fraud and Abuse Act (1986)	Primary federal statute used to combat computer crime.
Electronic Communications Privacy Act (1986)	Imposes fines and imprisonment for individuals who access, intercept, or disclose the private e-mail communications of others.
National Information Infrastructure Protection Act (1996)	Makes DoS attacks illegal; creates NIPC in the FBI.
Health Insurance Portability and Accountability Act (1996)	Requires certain health care facilities to report data breaches.
Financial Modernization Act (Gramm-Leach-Bliley Act) (1999)	Requires certain financial institutions to report data breaches.
Cyberspace Electronic Security Act (2000)	Reduces export restrictions.
Computer Security Enhancement Act (2000)	Protects federal government systems from hacking.
Electronic Signatures in Global and National Commerce Act (the "E-Sign Law") (2000)	Authorizes the use of electronic signatures in legal documents.
USA PATRIOT Act (2001)	Authorizes use of computer-based surveillance of suspected terrorists.
Homeland Security Act (2002)	Authorizes establishment of the Department of Homeland Security, which is responsible for developing a comprehensive national plan for security of the key resources and critical infrastructures of the United States; DHS becomes the central coordinator for all cyberspace security efforts.
CAN-SPAM Act (2003)	Although primarily a mechanism for civil and regulatory lawsuits against spammers, the CAN-SPAM Act also creates several new criminal offenses intended to address situations in which the perpetrator has taken steps to hide his or her identity or the source of the spam from recipients, ISPs, or law enforcement agencies. Also contains criminal sanctions for sending sexually explicit e-mail without designating it as such.
U.S. SAFE WEB Act (2006)	Enhances FTC's ability to obtain monetary redress for consumers in cases involving spyware, spam, Internet fraud, and deception; also improves FTC's ability to gather information and coordinate investigations with foreign counterparts.
Improving Critical Infrastructure Cybersecurity Executive Order (2013)	After Congress failed to pass cybersecurity legislation in 2012, this executive order issued by the Obama administration directs federal agencies to share cybersecurity threat intelligence with private sector companies that may be targets, and the development and implementation of a cybersecurity framework for private industry, incorporating best practices and voluntary standards.
Cybersharing Information Sharing Act (2015)	Encourages businesses and the federal government to share cyber threat information in the interests of national security,

devoted to tracking down criminal organizations and individuals engaged in attacks against Internet and e-commerce sites. On the federal level, the Office of Cybersecurity and Communications (CS&C) within the U.S. Department of Homeland Security (DHS) is responsible for overseeing the security, resilience, and reliability of the United States' cyber and communications infrastructure. The National Cybersecurity and Communications Integration Center (NCCIC) acts as a 24/7 cyber monitoring, incident response, and management center. In addition, the DHS also operates the **United States Computer Emergency Readiness Team (US-CERT)**, which coordinates cyber incident warnings and responses across both the government and private sectors. One of the better-known private organizations is the **CERT Coordination Center** (formerly known as the Computer Emergency Response Team) at Carnegie Mellon University. CERT monitors and tracks online criminal activity reported to it by private corporations and government agencies that seek out its help. CERT is composed of full-time and part-time computer experts who can trace the origins of attacks against sites despite the complexity of the Internet. Its staff members also assist organizations in identifying security problems, developing solutions, and communicating with the public about widespread hacker threats. The CERT Coordination Center also provides product assessments, reports, and training in order to improve the public's knowledge and understanding of security threats and solutions.

US-CERT

division of the U.S. Department of Homeland Security that coordinates cyber incident warnings and responses across government and private sectors

CERT Coordination Center

monitors and tracks online criminal activity reported to it by private corporations and government agencies that seek out its help

Government Policies and Controls on Encryption

In the United States, both Congress and the executive branch have sought to regulate the uses of encryption and to restrict availability and export of encryption systems as a means of preventing crime and terrorism. At the international level, four organizations have influenced the international traffic in encryption software: the Organization for Economic Cooperation and Development (OECD), G-7 (the heads of state of the top seven industrialized countries in the world, not including Russia, which was suspended from participation in 2014), the European Council, and the Wassenaar Arrangement (which includes 41 countries that produce sensitive industrial equipment or weapons). Various governments have proposed schemes for controlling encryption software or at least preventing criminals from obtaining strong encryption tools (see **Table 5.7**). The U.S. and U.K. governments are also devoting a large amount of resources to cryptography-related programs that will enable them to break encrypted communications collected on the Internet. Documents leaked by former NSA contractor Edward Snowden indicate that both the NSA and its U.K. counterpart, the GCHQ, may be able to break encryption schemes used by SSL/TLS, VPNs, and on 4G smartphones (Vaughan-Nichols, 2013). In recent years, the fight between the U.S. government and technology companies over encryption has shifted to the mobile platform, with Apple resisting U.S. government efforts to break Apple's iCloud and Apple iPhone encryption systems (see the Chapter 8 *Insight on Society* case, *Apple: Defender of Privacy?*) and concerns over encryption messaging apps such as WhatsApp, Signal, and Telegram, that offer end-to-end encryption for texts, photos, and videos that make it difficult, if not impossible, for authorities to intercept communications using such services (Isaac, 2016).

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.

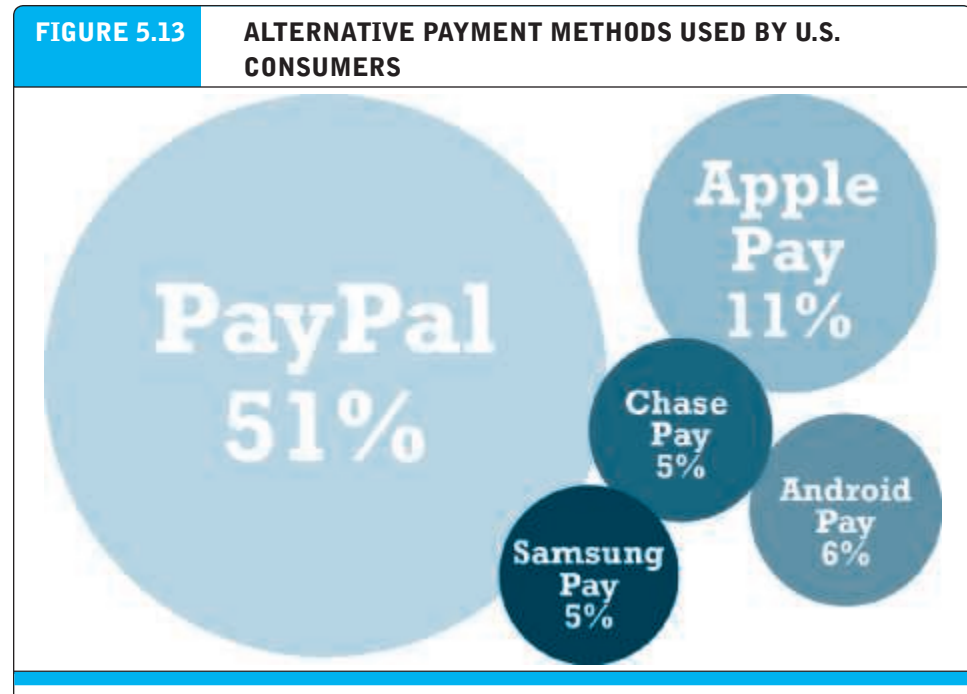
5.5 E-COMMERCE PAYMENT SYSTEMS

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.



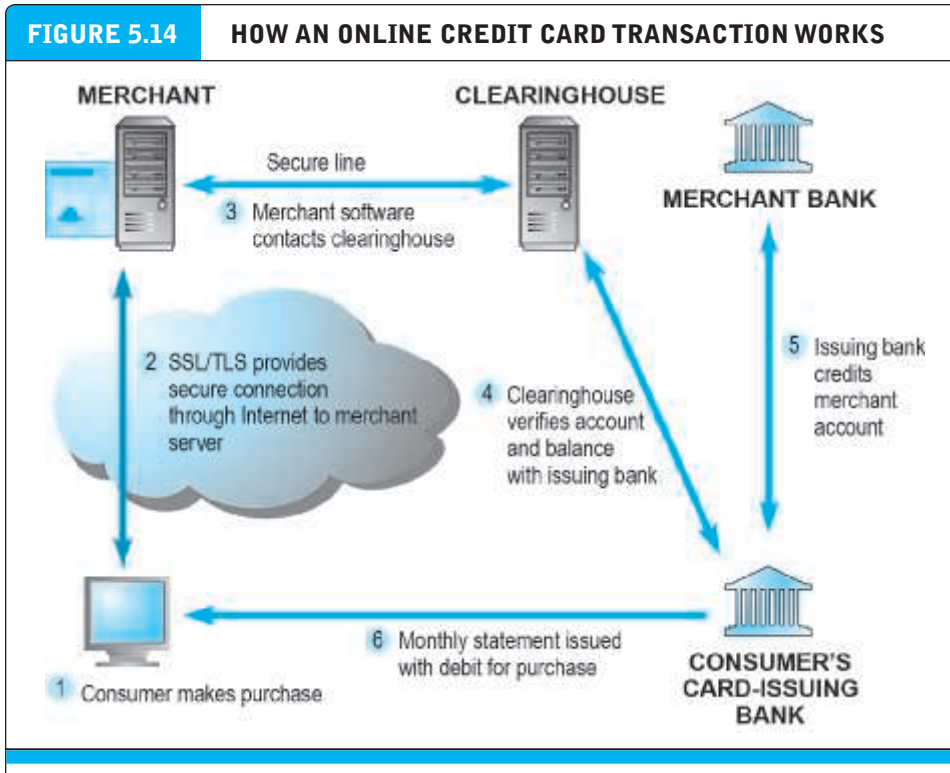
PayPal is still, by far, the most popular alternative payment method.

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

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

PCI-DSS (Payment Card Industry-Data Security Standards)

data security standards instituted by the five major credit card companies

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.

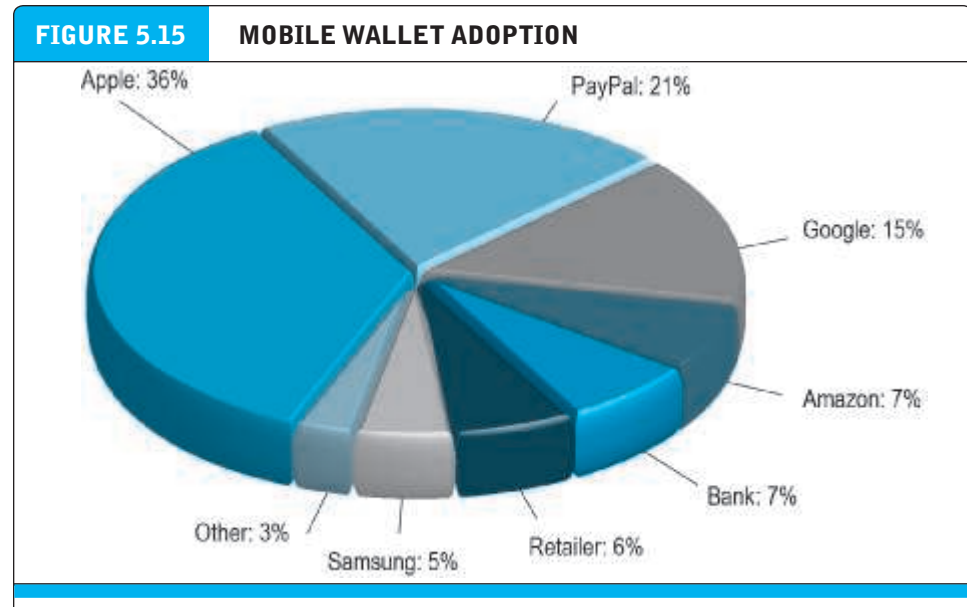
Near field communication (NFC) is the primary enabling technology for mobile payment systems. **Near field communication (NFC)** is a set of short-range wireless technologies used to share information among devices within about 2 inches of each other (50 mm). NFC devices are either powered or passive. 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,



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 cyber-criminals 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.

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.

digital cash

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

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-

INSIGHT ON BUSINESS

BITCOIN



In recent years, a number of countries around the world have experienced banking crises, eroding trust in the system. Enter Bitcoin, a form of electronic currency that can be transferred from one person to another via peer-to-peer networks, without the need for a bank or other financial institution as intermediary. This ability to operate outside the banking system has made Bitcoin a favorite of hackers and buyers and sellers of illicit goods and services; but more recently, it has made Bitcoin a darling among many in the technological elite who believe that Bitcoin and the technology behind it could be the next big thing in the payments industry.

Bitcoin has many unique attributes that differentiate it from traditional currencies. Bitcoins are not physically minted, but are generated by computer software at a predetermined rate beginning in 2009. A finite amount of coins are “built into the software,” such that in the year 2140, all of the coins will be mined and present in the market. The program that is used to generate Bitcoins runs on a peer-to-peer network and requires powerful computer systems to operate. “Mining” a Bitcoin is the result of these powerful computers solving cryptographic problems in tandem with other similar computers—the computer that hits upon the solution is awarded the coin, and a record of all of the involved computers’ attempts at mining the coin is logged. Bitcoins derive some of their initial value because of the time and computational effort required to mine them.

There are, however, many reasons to be skeptical of Bitcoin. Although law enforcement has improved its ability to apprehend criminals using Bitcoin, including the founder of the online black market Silk Road in 2015, governments are justifiably concerned about the emergence of a new currency without any tangible form whose purpose

is to avoid regulation. Bitcoin has also been lauded for its democratic structure, under which anyone running the underlying software has a say in making future changes. However, in 2016, Bitcoin is embroiled in a bitter civil war. As the currency continues to gain in popularity, limits on the Bitcoin transactions that can be processed each second, originally imposed as a safeguard, have begun to create backlogs and cripple transaction speed. Some of Bitcoin’s long-time supporters want to raise these limits to bring Bitcoin processing speed in line with services like PayPal; others argue that doing so could abandon the decentralized nature of the currency and place Bitcoin in the control of the few companies with the computing power to handle such a significant load, and out of the hands of the people. In 2016, there are now competing versions of Bitcoin, one which has removed transaction limits, and the other which remains faithful to the currency’s original vision, poor processing speed notwithstanding. Because of Bitcoin’s uncertainties and legal quandaries, the governments of many countries, including China, Denmark, Russia, and Israel, have taken a firm stand against digital cash.

Each of these developments has put downward pressure on Bitcoin’s value and slowed its growth, although Chinese exchanges accounted for 42% of all Bitcoin transactions in 2016, suggesting that China’s attempts to limit Bitcoin’s usage have been unsuccessful. A 2015 analysis of Bitcoin usage suggested that Bitcoins are still used primarily for gambling, illicit goods, and hoarding by speculators. Security concerns have also ravaged the largest Bitcoin exchanges to date, including Mt. Gox and Flexcoin. Hackers stole \$425 million and \$600,000 in Bitcoins from the two exchanges, respectively, and in 2016 the identity of the thieves and location of the Bitcoins stolen from Mt. Gox is still shrouded in mystery. These regulatory pressures and security concerns have driven Bitcoin’s dizzying volatility.

In 2012, Bitcoin's value was \$6; in 2013, it rose to \$1,200; and in 2016, it has surged back to \$650 after plummeting to nearly \$200 in 2015.

Despite all of these drawbacks, Bitcoin continues to move forward, and more banks and regulators are recognizing that the underlying technology may be here to stay. In 2015, Goldman Sachs invested heavily in Circle Internet Financial, a Bitcoin peer-to-peer payment platform, noting that Bitcoin could gain international acceptance over time. In September 2015, New York issued the first license to operate a virtual currency business, called a BitLicense, to Circle Internet, giving it the right to operate in the state, while subjecting it to strict capital, consumer protection, and anti-money laundering requirements. Many large U.S. banks, the New York Stock Exchange, Japanese telecom giant DoCoMo, the Bank of Tokyo, and other companies have invested in Coinbase, an intermediary for Bitcoin transactions. The first Bitcoin bank and the first Bitcoin investment fund launched in 2015 and the IRS began taxing Bitcoin earnings, further legitimizing it in the eyes of regulators. The EU, Japan, and a host of other countries proposed rules for the regulation, use, and trading of virtual currencies in 2016.

Companies like Circle Internet Financial hope to harness Bitcoin's decentralized network of computers to enable frictionless and inexpensive movement of currencies across international borders. Bitcoins and Bitcoin transactions are all logged on a public ledger known as the block-

chain, which is updated and maintained by all of the members of the network. Contrast this with a bank, which is a central hub where all currency and financial information resides. With the blockchain, there isn't a single point of failure or vulnerability the way there may be with a bank, and no single entity must update and maintain the ledger. For Bitcoin to truly gain acceptance, regular people will need to begin using it for everyday transactions. In countries where the banking system is less developed than in the United States, this has already begun to happen. In Argentina, the Philippines, Kenya, and other similar countries, banking regulations have made Bitcoin a more appealing alternative for ordinary people making normal commercial transactions.

A number of high-profile online businesses accept Bitcoin, such as Dell, Microsoft Expedia, and Newegg, as well as reportedly over 80,000 other merchants around the world. Bitcoin trading volume is still down significantly from its peak in 2014, but by July 2016, volume had spiked up again. Industry analysts predict that the number of active Bitcoin users will grow to 4.7 million in 2019, up from roughly 1.3 million today. Analysts also believe that the number of transactions per day will grow to 200,000 per day in 2016, with a value of more than \$92 billion, up from \$27 billion in 2015. For Bitcoin to continue to grow, however, it must become more than just a trading commodity and prove itself to be a useful tool to actually purchase goods and services.

SOURCES: "Coinbase Eyes Japan Expansion After Landing Investment from Bank of Tokyo," by Jon Russell, Techcrunch.com, July 8, 2016; "EU Proposes Stricter Rules on Bitcoin, Prepaid Cards, Terrorism Fight," by Foo Yun Chee, Reuters.com, July 5, 2016; "How China Took Center Stage in Bitcoin's Civil War," by Nathaniel Popper, *New York Times*, June 29, 2016; "Bitcoin Transactions Values to Triple This Year, Reaching Over \$92BN," by Juniper Research, June 4, 2016; "Bitcoin Is on the Verge of Splitting in Two," by Ben Popper, Theverge.com, February 9, 2016; "Mt. Gox Creditors Seek Trillions Where There Are Only Millions," by Nathaniel Popper, *New York Times*, May 25, 2016; "We Must Regulate Bitcoin. Problem Is, We Don't Understand It," by Primavera De Filippi, Wired.com, March 1, 2016; "A Bitcoin Believer's Crisis of Faith," by Nathaniel Popper, *New York Times*, January 14, 2016; "Bitcoin's Big Challenge in 2016: Reaching 100 Million Users," by Michael Jackson, Coindesk.com, January 1, 2016; "Circle Gets First 'BitLicense,' Releases Circle Pay, New Service," by Paul Vigna, *Wall Street Journal*, September 22, 2015; "Goldman and IDG Put \$50 Million to Work in a Bitcoin Company," by Nathaniel Popper, *New York Times*, April 30, 2015; "Bitcoin Behemoth Coinbase launches in the UK," by Alex Hern, *The Guardian*, April 29, 2015; "The World's First Proper Bitcoin Exchange Will Go Live in a Month," by Kieren McCarthy, *The Register*, April 29, 2015; "Final New York Bitcoin Regulation Released: BitLicense," by P.H. Madore, Cryptocoins.com, April 6, 2015; "Bitcoin's Golden Moment: BIT Gets FINRA Approval," by Brian Kelly, Cnbc.com, March 4, 2015; "Tokyo Court: Bitcoin Exchange Mt. Gox Will Liquidate," by Donna Leinwand, *USA Today*, April 16, 2014; "China Cracks Down on Bitcoin," by Chao Deng and Lingling Wei, *Wall Street Journal*, April 1, 2014; "The Mt. Gox Bitcoin Scandal Is the Best Thing to Happen to Bitcoin in Years," by Heidi Moore, Theguardian.com, February 26, 2014; "Israel's Central Bank Warns on Potential Fraud With Bitcoin," by Calev Ben-David, Bloomberg.com, February 19, 2014; "Russian Authorities Say Bitcoin Illegal," by Gabriela Baczynska, Reuters.com, February 9, 2014; "Bitcoin Pitchman Busted for 'Selling \$1M in Currency to Silk Road,'" by Kaja Whitehouse and Rich Calder, *New York Post*, January 27, 2014; "Following the Bitcoin Trail," Economist.com, August 28, 2013.

**electronic billing
presentment and
payment (EBPP)
system**

form of online payment
system for monthly bills

tances. The billing market represents an extraordinary opportunity for using the Internet as an electronic billing and payment system that potentially could greatly reduce both the cost of paying bills and the time consumers spend paying them. Estimates vary, but online payments are believed to cost between only 20 to 30 cents to process.

Electronic billing presentment and payment (EBPP) systems are systems that enable the online delivery and payment of monthly bills. EBPP services allow consumers to view bills electronically using either their desktop PC or mobile device and pay them through electronic funds transfers from bank or credit card accounts. More and more companies are choosing to issue statements and bills electronically, rather than mailing out paper versions, especially for recurring bills such as utilities, insurance, and subscriptions.

MARKET SIZE AND GROWTH

In 2002, 61% of bill payments were made by check, and only 12% by online bill payments. In 2015, in contrast, online bill payments accounted for more than 55% of all bill payments, while paper checks now account for less than 20%. Among online households, almost three-quarters pay at least one bill online each month, and almost half receive at least one bill electronically each month. Mobile bill payments are surging, with 33% U.S. households in 2015 paying at least one bill on a mobile device. Most consumers cited the convenience and time saved by using mobile bill payment (Fiserv, 2016).

One major reason for the surge in EBPP usage is that companies are starting to realize how much money they can save through online billing. Not only is there the savings in postage and processing, but payments can be received more quickly (3 to 12 days faster, compared to paper bills sent via regular mail), thereby improving cash flow. Online bill payment options can also reduce the number of phone calls to a company's customer service line. In order to realize these savings, many companies are becoming more aggressive in encouraging their customers to move to EBPP by instituting a charge for the privilege of continuing to receive a paper bill.

Financials don't tell the whole story, however. Companies are discovering that a bill is both a sales opportunity and a customer retention opportunity, and that the electronic medium provides many more options when it comes to marketing and promotion. Rebates, savings offers, cross-selling, and upselling are all possible in the digital realm, and much less expensive than mailed envelopes stuffed with offers.

EBPP BUSINESS MODELS

There are four EBPP business models: online banking, biller-direct, mobile, and consolidator.

The online banking model is the most widely used today. Consumers share their banking or credit card credentials with the merchant and authorize the merchant to charge the consumer's bank account. This model has the advantage of convenience for the consumer because the payments are deducted automatically, usually with a notice from the bank or the merchant that their account has been debited.

In the biller-direct model, consumers are sent bills by e-mail notification, and go to the merchant's website to make payments using their banking credentials. This

model has the advantage of allowing the merchant to engage with the consumer by sending coupons or rewards. The biller-direct model is a two-step process, and less convenient for consumers.

The mobile model allows consumers to make payments using mobile apps, once again relying on their bank credentials as the source of funds. Consumers are notified of a bill by text message and authorize the payment. An extension of this is the social-mobile model, where social networks like Facebook integrate payment into their messaging services. The mobile model has several advantages, not least of which is the convenience for consumers of paying bills while using their phones, but also the speed with which bills can be paid in a single step. This is the fastest growing form of EBPP. In 2016, Facebook and PayPal announced a deal in which Facebook users can pay for purchases on Facebook using PayPal (Demos, 2016). Consumers will not have to leave Facebook in order to purchase and pay for products.

In the consolidator model, a third party, such as a financial institution or a focused portal such as Intuit's Paytrust, Fiserv's MyCheckFree, Mint Bills, and others, aggregates all bills for consumers and permits one-stop bill payment. This model has the advantage of allowing consumers to see all their bills at one website or app. However, because bills come due at different times, consumers need to check their portals often. The consolidator model faces several challenges. For billers, using the consolidator model means an increased time lag between billing and payment, and also inserts an intermediary between the company and its customer.

Supporting these primary business models are infrastructure providers such as Fiserv, Yodlee, FIS Global, ACI Worldwide, MasterCard RPPS (Remote Payment and Presentment Service), and others that provide the software to create the EBPP system or handle billing and payment collection for the biller. **Figure 5.16** categorizes the major players in the EBPP marketplace.



The main business models in the EBPP marketplace are biller-direct, online banking, consolidator, and mobile. Infrastructure providers support all of these competing models.

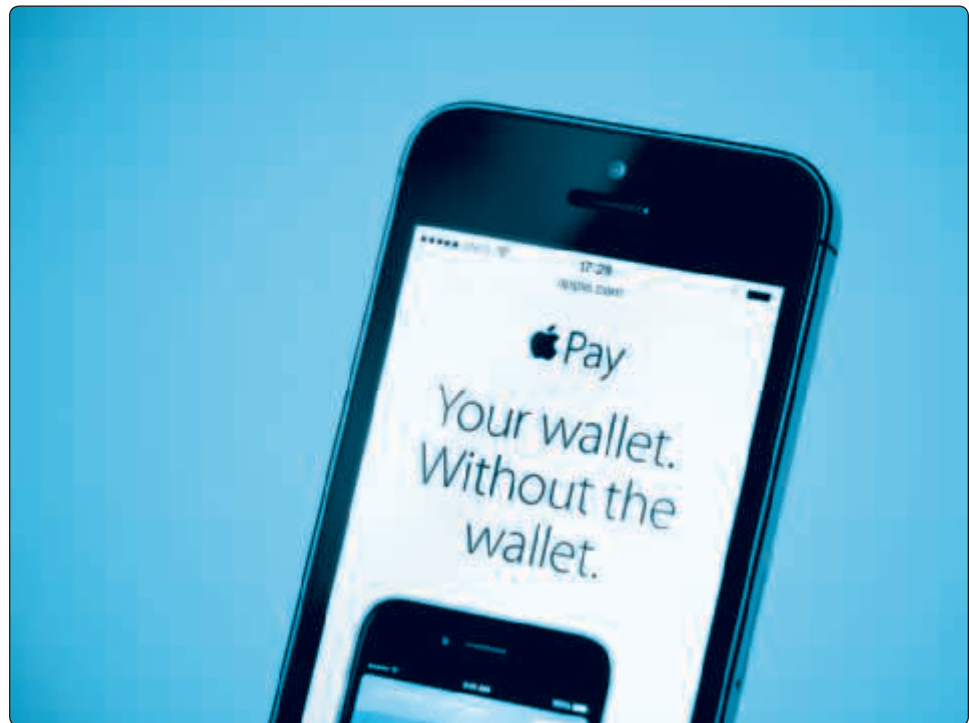
5.7

CASE STUDY

The Mobile Payment Marketplace:

Goat Rodeo

Nearly every day, it seems, a new mobile payment system is announced by giant tech companies, startups, merchants, and banks. The mobile payment marketplace is experiencing an explosion of innovative ideas, plans, and announcements, which one commentator has likened to a goat rodeo, a chaotic situation in which powerful players with different agendas compete with one another for public acceptance, and above all, huge potential revenues. The mobile payment market is expected to generate somewhere between \$27 billion and \$75 billion in transaction volume in 2016, more than doubling the 2015 number. This wide-range estimate indicates how little is really known about the size of mobile payments, except that they are rapidly growing, especially among Millennials who have stopped using checks, and unlike their parents, are comfortable handling their financial trans-



actions and banking using a smartphone. Times are changing: for the first time, more people are using mobile banking on their phones and laptops than going to a bank branch.

American consumers spent over \$5.1 trillion on credit and debit card transactions in 2015, and mobile payments are still just a tiny percentage of the existing credit and debit card system. But even if a small percentage of the \$5 trillion credit card transactions move from plastic to mobile, the potential revenue is very large. On the other hand, moving consumers away from over 800 million credit and debit cards, which can be swiped at millions of merchants and used online with ease and safety, is proving to be a difficult task. The rosy future of mobile payments painted by tech companies may be a long time coming.

The mobile payment market is a battle among the titans of online payment and retailing: PayPal, credit card companies like Visa and MasterCard, Google, Apple, Samsung, and startup tech companies like Venmo and Square. The startups are backed by millions in venture capital. Even large retailers like Walmart, Best Buy, and Target are getting into the game by developing their own mobile payment apps. Major banks are in the line of fire: who needs a checking account when you can pay with a mobile phone? Rising to this challenge, the banks are slowly building their own mobile payment systems, and investing in startups to lead the charge.

There are, by one count, already about 8,000 startups in the mobile payment market. The most recent startups focus on peer-to-peer mobile payments. Venmo is a good example. Venmo is a social-mobile payment app that lets users transfer money to one another. It can also be used to pay at a small number of participating merchants. Founded in 2010 by two college students who wanted to send cash to one another for sharing restaurant tabs and paying small debts without the hassle of cash or writing checks, Venmo was purchased by PayPal in 2013. Users sign up for a Venmo account and link their account to a bank account, a debit card, or credit card. Users can also create a Venmo balance by sending money to their Venmo account, and then charge payments against that balance. There is no charge for the service when users have a Venmo balance or use a debit card, and a 3% charge for using a credit card as the source of funds. There is a social aspect of Venmo that allows users to share their purchase events (but with amount paid stripped from the notification). Users have the option to keep all transactions private as well. When they want to make a payment to another person, they enter the person's e-mail and the funds are transferred when the recipient, who must also have a Venmo account, accepts the payment. Venmo relies on NFC technology to make in-person payments to individuals by tapping their phones. Venmo's popularity has skyrocketed, especially among Millennials, and in January 2016 it processed \$1 billion in transactions, a 250% increase over the previous year. The company does not release information on its subscriber base, and because it is largely a free service, it does not contribute significantly to PayPal's gross revenues. PayPal has begun to monetize its investment in Venmo by expanding beyond peer-to-peer small payments, and extending its use to merchants who accept PayPal payments, a much larger user base, which includes large retailers like Home Depot, Target, Sears, and OfficeMax.

Startups like Venmo are small fry compared to the three other giants in the mobile payment market. First in terms of subscribers are the technology companies like

Apple, Google, Samsung, PayPal, and Square, all of which have major hardware and software mobile payment initiatives. Apple, Google, and Samsung own and license the hardware and software platform of the ubiquitous smartphone, while PayPal and Square operate large-scale payment processing platforms. Second, the large national merchants are developing their own mobile payment systems in an effort, in part, to sidestep the credit card companies (Visa, MasterCard, Discover, and American Express), which charge them a 3% transaction fee that gets passed along to the consumer as 3% higher prices, and in part to maintain control over the point-of-sale consumer moment at the cash register. These firms have tens of millions of loyal customers. Banks like JPMorgan Chase, Wells Fargo, Citi, and other money center banks, and of course, the credit card companies Visa, Master Card, and others, are the third major player. These firms have the advantage of owning and operating the global banking and credit card systems, with hundreds of millions of loyal banking and credit card customers, and the expertise to provide security and financial stability for their products. They are, however, very slow movers and are just now entering the mobile payment marketplace.

Let's take a look at the technology companies first, all of whom offer variations on contactless payments, often referred to as digital or mobile wallets. Apple Pay is an app that comes with iPhone 6 phones and later. It uses built-in NFC technology. Users set up an account, and enter their banking credentials, using either their credit/debit card account information, or their checking or savings account, as the source of funds.

When a customer wants to make a payment, he or she presses the iPhone Touch ID button, which reads the customer's fingerprint and ensures the phone does indeed belong to the person. On the Apple Watch, there's a special button just for Apple Pay transactions. Next, the consumer swipes the device near a merchant's NFC point-of-sale terminal, which begins the transaction process. The iPhone 6 and later comes with a hardware-defined secure area on a chip that contains a unique device number and the ability to generate a one-time 16-digit code. Together they form a digital token. The token information is encrypted and sent to Apple servers to verify the authenticity of the device and the person. Apple sends the payment request to the credit card issuer. Credit card issuers verify the account owner and available credit. In about one second, the transaction is approved or denied. Credit card information is not shared with the merchant and not transmitted from the iPhone. The 800 million credit cards stored on Apple's servers are also encrypted. If hackers intercept the NFC communication at the point-of-sale, or intercept the stream of data moving over the cellular network, it would be useless, and incapable of supporting additional transactions because the message is encrypted, and involves a one-time-only digital token.

Apple Pay is free to consumers, and the credit card companies charge their usual fee of 3% for each transaction. Apple collects .15% from the credit companies and banks, and in return, guarantees the transaction is valid. Apple Pay does not store any user funds and is solely a technology-based intermediary between consumers and banks, and, unlike Venmo, is not subject to federal banking regulations. Merchants' point-of-sale terminals need to be NFC-enabled, and merchants need to install Apple software to accept payments. Apple Pay can be used by any consumer that has a credit card from a major issuer bank.

Apple has developed relationships with many of the key players in the payment ecosystem, including credit giants Visa, MasterCard, American Express, and Discover, as well as 11 large bank credit card issuers including JPMorgan Chase, Bank of America, Citigroup, and Wells Fargo, which together account for 83% of U.S. credit card payment volume. Apple has also signed up national merchants such as Walgreens, Duane Reade, McDonald's, Disney, Macy's, Bloomingdale's, Staples, and Whole Foods. Groupon and Uber have integrated Apple Pay into their systems.

Android Pay is a Google app that provides an NFC-based payment system much like Apple Pay. Android is the most widely used smartphone operating system in the world. Launched in 2015, Android Pay replaces Google Wallet, which has been repurposed as a peer-to-peer payment service that allows users to pay friends using only their e-mail address, similar to PayPal and Venmo. Users sign up for an Android Pay account by entering their existing bank credit or debit card account information, or by depositing a prepaid balance of funds in their Android Pay account. Google is for some users a prepaid digital card where users transfer funds to their Android Pay account, and therefore is subject to federal regulations. To use Android Pay, customers hold their phone near the merchant's NFC terminal at checkout. Users are asked to enter their PIN and then choose to pay with either the credit or debit card on file with Android Pay or with their cash balance. If the user chooses to pay with a bank card, the app creates a unique digital token and sends this as an encrypted message to Android servers, which then communicate with the issuing bank, for approval. Approval messages are sent to the merchant's point-of-sale terminal. No card information is transmitted from the point of purchase. Android Pay is free for subscribers except when they use their credit card, which entails a 3% credit card transaction fee charged by the credit card companies. However, Google may offer consumers rewards, and in the future, display ads. Because Android Pay can store user funds, it is subject to federal banking regulations.

Samsung Pay was introduced by Samsung in the United States in September 2015, after an earlier roll-out in Samsung's home country, South Korea. Samsung smartphones are the most widely used smartphones in the world. As with Apple Pay and Android Pay, users create an account, and submit their bank credit or debit card information. Samsung Pay prioritizes the use of NFC technology when merchants have the appropriate terminal, but when that is not available, switches to a technology called Magnetic Secure Transmission that sends the card data stored on the user's device to traditional magnetic stripe terminals. This means that Samsung Pay can be used by the millions of existing point-of-sale card swiping terminals without upgrading to NFC terminals or installing any apps. Samsung Pay also stores coupons and reward cards, but does not store user funds and is not a prepaid card. Therefore, it most likely will not be subject to U.S. federal regulations. Like the other mobile wallets, it is essentially a place where users can store all their credit cards.

Currently, the most popular mobile payment systems are offered by PayPal and Square, some of which do not use NFC. While claiming to be financial services firms, both PayPal and Square are financial service software platform firms, technology companies in disguise. PayPal was late to the mobile payment market, beaten to the punch by Square. Square started in 2009 with Square Reader, a square plastic device

that plugged into an iPhone or iPad, and allowed users to easily set up a merchant license to accept credit cards, and then swipe the cards locally on the Square Reader device. Using the Square app, it allows merchants to easily accept credit card payments from customers on the go. Square also developed Square Register (now called Point of Sale), which is a software app that turns a tablet into a point-of-sale terminal and cash register. Square has morphed into a small business services company, serving coffee shops, newsstands, small retailers, and farmers' market merchants, as well as piano teachers, baby sitters, and taxi drivers, allowing them to easily accept credit card payments. Square generated \$1 billion in revenue in 2015, and showed a loss of \$174 million.

PayPal is currently the most successful and profitable non-traditional online payment system, used mostly on desktops and tablets, but rapidly becoming a mobile payment force. PayPal is currently the largest alternative (non-credit card) online payment service, processing \$282 billion in transactions in 2015, and has 188 million subscribers. PayPal processed \$66 billion in mobile payments in 2015, up from \$27 billion in 2013. PayPal is growing payment volume at around 20% annually.

PayPal currently enables mobile payments in three ways. First, PayPal sells a device that allows merchants (mostly small businesses) to swipe credit cards using a smartphone or tablet, just like the Square device. Second, the most common PayPal mobile payment occurs when customers use their mobile device browser on a tablet or smartphone to make a purchase or payment at a website. This is not very helpful for merchants like Starbucks, Macys, or local restaurants, who would like customers to be able to purchase goods in their stores and outlets on the fly without keying in information to a smartphone. A third method is PayPal's updated app for iOS and Android devices. On entering a merchant's store that accepts PayPal app payments, the app establishes a link using Bluetooth with the merchant's app that is also running on an iOS or Android device. This step authenticates the user's PayPal account. On checkout, the customer tells the merchant he or she will pay with PayPal. The merchant app charges the customer's PayPal account. After the payment is authorized, a message is sent to the customer's phone. No credit card information is being transmitted or shared with the merchant. Users do not have to enter a pin code or swipe their phone at a special merchant device, so merchants are not required to purchase an expensive NFC point-of-sale device, but they must have the PayPal merchant app stored on a PC which is really acting like a digital cash register. In 2012, PayPal launched PayPal Here, a device that will both read credit cards equipped with computer chips, as well as accept payments from Android Pay and Apple Pay. The service includes a card reader that plugs into a tablet or smartphone, and a stand-alone contactless device that can accept NFC payments, as well as swipe credit cards. In 2015, PayPal launched the PayPal.me app, a peer-to-peer payment service that allows users to make and receive payments from friends. Users share their PayPal.me link with friends and can transfer money to their PayPal accounts. The service is free and is a direct competitor with Venmo and other P2P payment services. Venmo, which PayPal also owns, only works with U.S. banks, credit and debit cards, while PayPal.me is targeted at PayPal's global user base. In 2016 PayPal launched NFC payments for locations that accept VISA's contactless payments.

SOURCES: "Consumer Bill Payments Shifts & Strategies," by Jim Gilligan and Kellie Thomas, Payments.com, 2016; "PayPal Gets Friendlier With Facebook," by Telis Demos, *New York Times*, October 24, 2016; "Apple Pay at Two Years: Not Much to Celebrate (Yet)," by Mark Hamblen, Computerworld.com, October 20, 2016; "How Millennials Became Spooked by Credit Cards," by Nathaniel Popper,

While mobile payment systems developed by technology companies are experiencing rapid growth, mobile wallets developed by large national merchants have sputtered. Large national merchants have had a contentious relationship with credit card firms because of the 3% fees charged by credit card companies, which raise prices to consumers by the same amount. Merchants would much prefer customers pay with store credit cards that are linked to the customer's bank account, or debit accounts, where banks do not charge a fee, or customer-supplied prepayment funds. Some merchants also offer their own store credit cards and have developed their own transaction processing systems, circumventing the bank credit card system entirely. Merchants also want to control the point-of-sale moment, where they can offer coupons, loyalty rewards, and special discounts, rather than rely on mobile wallets provided by the technology companies, which do not offer these capabilities.

In 2012, a joint venture of the 15 largest merchants announced the Merchant Customer Exchange (MCX). MCX was backed by Walmart, Target, Sears, 7-Eleven, Sunoco, and 10 other national pharmacies, supermarkets, and restaurant chains. The backers of this effort have annual sales of more than \$1 trillion dollars. That was enough to make everyone involved in mobile payments stand up and listen, even Google and Apple. Their initial effort was coined CurrentC, and was piloted in 2014. CurrentC was an app that allowed customers to pay using their bank accounts, bank debit cards, or store-issued credit cards, but not traditional bank credit cards. The idea was to circumvent the bank credit system entirely, and avoid paying the credit companies their typical 3% fee. CurrentC was withdrawn in 2016, and the MCX joint venture has ended due to squabbles among the partners, and an excessively long development time for the app. In 2016, Walmart introduced its own Walmart Pay app for both iOS and Android phones. Using QR recognition technology, not NFC, Walmart Pay now accepts all bank credit and debit cards, as well as Walmart store credit cards. It can also read coupons and offer rewards to loyal customers. Walmart Pay can only be used at Walmart stores, but given that Walmart has 140 million customers a week in the United States, that's not a terrible disadvantage. As of October 2016, 22 million customers are using the Walmart Pay app every month. The advantage to Walmart is that it owns the customer transaction, and information, without the intervention of the tech giants. Walmart, and the other large national merchants, will have to live with the credit card companies and their 3% fees for now.

The third entrant to the mobile payment market is composed of the large national banks and credit card companies. Banks and credit card firms have been very slow moving into the mobile payment space, in part because the existing credit system works so well and their cards are widely accepted by consumers and merchants. Mobile payment systems from tech companies and merchants are competitors for the loyalty of bank customers who deposit billions of dollars in bank checking, savings, and debit cards, where banks can charge fees, and use the deposits essentially free of cost, given the low or non-existent interest rates on these accounts. JP Morgan Chase has launched Retail Checkout, a card reader that accepts tap card and mobile wallet NFC payments, and the Chase Mobile app for smartphones and tablets, which allows bank customers to perform a wide variety of banking functions like peer-to-peer payments by e-mail (QuickPay), pay bills, deposit checks, check balances, and even apply for

New York Times, August 14, 2016; "Under Pressure, Big Banks Vie for Instant Payment Market," by Michael Corkey, *New York Times*, August 1, 2016; "PayPal to Roll Out NFC Mobile Payments Across the US Through Visa Deal," by Rian Boden, *NFCworld.com*, July 25, 2016; "Walmart Pay vs. Apple Pay: Hardware Age Dictates All," by Evan Shuman, *Computerworld.com*, July 8, 2016; "In Mobile Payments War, Big Banks Strike Back," by Aaron Black, *Wall Street Journal*, July 8, 2016; "The Mobile Payments Report," by Evan Baker, *Businessinsider.com*, June 3, 2016; "Reasons that US Smartphone Users Don't Use Mobile Payments," *eMarketer, Inc.*, June 2016; "Why Apple Pay and Other Mobile Wallets Beat Chip Cards," by Brian Chen, *New York Times*, May 4, 2016; "Apple Pay's Big Drop," *Pymnts.com*, March 18, 2016; "Latest Mobile-Banking Research Shows Laptops Still Reign," by Robin Sidel, *Wall Street Journal*, January 27, 2016; "As More Pay by Smartphone, Banks Scramble to Keep Up," by Steve Lohr, *New York Times*, January 18, 2016; "For the First Time, More Are Mobile-Banking Than Going to a Branch," by Telis Demos, *Wall Street Journal*, January 12, 2016; "US Mobile Payments Forecast," by Bryan Yeager, *eMarketer, Inc.*, November 2015; "Bold Bet That Banking Industry Is Poised for Serious Disruption," by Michael Casey, *Wall Street Journal*, June 5, 2015; "'Pretty Useless': Consumer Frustrations Grow Over New Credit Card Chip," by Alexandra Zaslowsky, *Todaymoney.com*, October 16, 2015; "Square's IPO Filing: It's Complicated," *Recode.net*, by Jason Del Rey, October 14, 2015; "PayPal Here Launches a Mobile Card Reader That Accepts Android Pay and Apple Pay," by Ruth Reader, *Venturebeat.com*, September 28, 2015; "Samsung Pay: What You Need to Know (FAQ)," by Lexy Savvides, *Cnet.com*, September 28, 2015; "Revamped Google Wallet Arrives on iOS," by Stephanie Mlot, *Pcmagazine.com*, September 22, 2015; "Apple Pay Competitor CurrentC May Not Launch Until Next Year," by Jason Del Rey, *Recode.net*, August 12, 2015;

"PayPal Returns to Market with \$52 Billion Valuation," by Devika Krishna Kumar and Mari Saito, Reuters.com, July 20, 2015; "There Are No Transaction Fees for Android Pay, Which Is Good for Us, Bad for Google," by Robert Nazarian, Digitaltrends.com, June 8, 2015; "The State of Mobile Payments in 2015," by James A. Martin, CIO.com, April 22, 2015; "Apple Sees Mobile-Payment Service Gaining in Challenge to PayPal," by Olga Kharif, Bloomberg.com, January 27, 2015; "What Apple Pay Means for Retailers," by Abby Callard, Internetretailer.com, September 12, 2014; "Apple Pay: No Charge for Merchants, But Transaction-Security Fees for Issuers," by Jim Daly, Digitaltransaction.net, September 11, 2014.

mortgages. Citi has launched Citi Mobile with similar functionality. Banks so far have not introduced apps for making NFC payments for consumer purchases, but these will surely be introduced shortly. The large banks are investing heavily in payment startups to acquire these capabilities.

The future for smartphone mobile wallets is assured given the size of the players involved, the potential rewards for successful players, and the demands of consumers for a payment system that does not involve swiping plastic cards, dealing with slips of paper receipts, and digging for cash in their pockets and purses.

But the transition is going much slower than pundits initially thought, with millions of consumers trying the new methods once, and then not using them again because not enough merchants accept them, lack of familiarity, and concerns about security and privacy. One recent study found there are now 11 million contactless mobile payment users in the United States, but just 2.3 million who are active users. It is unlikely that all the mobile payment systems described above will survive, and also quite likely that consumers will remain confused by all their payment options for some time yet to come. A full transition to mobile payments will be a long time coming.

Case Study Questions

1. Who are the three major players in the mobile payment market?
2. Why is Venmo considered a social-mobile payment system?
3. How does Apple Pay differ from Android Pay and Samsung Pay?
4. How does PayPal enable mobile payments?

5.8 REVIEW

KEY CONCEPTS

- Understand the scope of e-commerce crime and security problems, the key dimensions of e-commerce security, and the tension between security and other values.
- While the overall size of cybercrime is unclear, cybercrime against e-commerce sites is growing rapidly, the amount of losses is growing, and the management of e-commerce sites must prepare for a variety of criminal assaults.
- There are six key dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability.
- Although computer security is considered necessary to protect e-commerce activities, it is not without a downside. Two major areas where there are tensions between security and website operations are:
 - *Ease of use*—The more security measures that are added to an e-commerce site, the more difficult it is to use and the slower the site becomes, hampering ease of use. Security is purchased at the price

of slowing down processors and adding significantly to data storage demands. Too much security can harm profitability, while not enough can potentially put a company out of business.

- *Public safety*—There is a tension between the claims of individuals to act anonymously and the needs of public officials to maintain public safety that can be threatened by criminals or terrorists.

■ Identify the key security threats in the e-commerce environment

- The most common and most damaging forms of security threats to e-commerce sites include:
 - *Malicious code*—viruses, worms, Trojan horses, ransomware, and bot networks are a threat to a system's integrity and continued operation, often changing how a system functions or altering documents created on the system.
 - *Potentially unwanted programs (adware, spyware, etc.)*—a kind of security threat that arises when programs are surreptitiously installed on your computer or computer network without your consent.
 - *Phishing*—any deceptive, online attempt by a third party to obtain confidential information for financial gain.
 - *Hacking and cybervandalism*—intentionally disrupting, defacing, or even destroying a site.
 - *Credit card fraud/theft*—one of the most-feared occurrences and one of the main reasons more consumers do not participate in e-commerce. The most common cause of credit card fraud is a lost or stolen card that is used by someone else, followed by employee theft of customer numbers and stolen identities (criminals applying for credit cards using false identities).
 - *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.
 - *Spoofing*—occurs when hackers attempt to hide their true identities or misrepresent themselves by using fake e-mail addresses or masquerading as someone else.
 - *Pharming*—involves redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination.
 - *Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks*—hackers flood a website with useless traffic to inundate and overwhelm the network, frequently causing it to shut down and damaging a site's reputation and customer relationships.
 - *Sniffing*—a type of eavesdropping program that monitors information traveling over a network, enabling hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports. The threat of sniffing is that confidential or personal information will be made public.
 - *Insider jobs*—although the bulk of Internet security efforts are focused on keeping outsiders out, the biggest threat is from employees who have access to sensitive information and procedures.
 - *Poorly designed server and client software*—the increase in complexity and size of software programs has contributed to an increase in software flaws or vulnerabilities that hackers can exploit.
 - *Social network security issues*—malicious code, PUPs, phishing, data breaches, identity fraud, and other e-commerce security threats have all infiltrated social networks.
 - *Mobile platform security issues*—the mobile platform presents an alluring target for hackers and cybercriminals, and faces all the same risks as other Internet devices, as well as new risks associated with wireless network security.
 - *Cloud security issues*—as devices, identities, and data become more and more intertwined in the cloud, safeguarding data in the cloud becomes a major concern.

■ Describe how technology helps secure Internet communications channels and protect networks, servers, and clients.

- 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. Encryption can provide four of the six key dimensions of e-commerce security: message integrity, nonrepudiation, authentication, and confidentiality.

- There are a variety of different forms of encryption technology currently in use. They include:
 - *Symmetric key cryptography*—Both the sender and the receiver use the same key to encrypt and decrypt a message.
 - *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. Once the keys are used to encrypt a message, the same keys cannot be used to unencrypt the message.
 - *Public key cryptography using digital signatures and hash digests*—This method uses a mathematical algorithm called a hash function to produce a fixed-length number called a hash digest. 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 that the same result is produced. The sender then encrypts both the hash result and the original message using the recipient's public key, producing a single block of cipher text. To ensure both the authenticity of the message and nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender's private key. This produces a digital signature or “signed” cipher text that can be sent over the Internet to ensure the confidentiality of the message and authenticate the sender.
 - *Digital envelope*—This method uses symmetric cryptography to encrypt and decrypt the document, but public key cryptography to encrypt and send the symmetric key.
 - *Digital certificates and public key infrastructure*—This method relies on certification authorities who issue, verify, and guarantee digital certificates (a digital document 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, and other identifying information).
 - In addition to encryption, there are several other tools that are used to secure Internet channels of communication, including: Secure Sockets Layer (SSL)/Transport Layer Security (TLS), virtual private networks (VPNs), and wireless security standards such as WPA2.
 - After communications channels are secured, tools to protect networks, the servers, and clients should be implemented. These include: firewalls, proxies, intrusion detection and prevention systems (IDS/IDP), operating system controls, and anti-virus software.
- **Appreciate the importance of policies, procedures, and laws in creating security.**
- In order to minimize security threats, e-commerce firms must develop a coherent corporate policy that takes into account the nature of the risks, the information assets that need protecting, and the procedures and technologies required to address the risk, as well as implementation and auditing mechanisms.
 - Public laws and active enforcement of cybercrime statutes also are required to both raise the costs of illegal behavior on the Internet and guard against corporate abuse of information.
 - The key steps in developing a security plan are:
 - *Perform a risk assessment*—an assessment of the risks and points of vulnerability.
 - *Develop a security policy*—a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets.
 - *Create an implementation plan*—a plan that determines how you will translate the levels of acceptable risk into a set of tools, technologies, policies, and procedures.
 - *Create a security team*—the individuals who will be responsible for ongoing maintenance, audits, and improvements.
 - *Perform periodic security audits*—routine reviews of access logs and any unusual patterns of activity.
- **Identify the major e-commerce payment systems in use today.**
- The major types of e-commerce payment systems in use today include:

- *Online credit card transactions*, which are the primary form of online payment system. 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. However, the online credit card system has a number of limitations involving security, merchant risk, cost, and social equity.
 - *PayPal*, which is an example of an alternative payment system that permits consumers to make instant, online payments to merchants and other individuals based on value stored in an online account. Other examples include Pay with Amazon, Visa Checkout, MasterPass, Bill Me Later, and WU Pay.
 - *Mobile payment systems*, which use either credit card readers attached to a smartphone (Square, PayPal Here) or near field communication (NFC) chips, which enable mobile payment at point-of-sale (Apple Pay, Android Pay, and Samsung Pay).
 - *Digital cash*, such as Bitcoin and virtual currencies. Digital cash is growing in importance and can be used to hide payments from authorities, as well as support the legitimate exchange of value.
- Describe the features and functionality of electronic billing presentment and payment systems.
- Electronic billing presentment and payment (EBPP) systems are a form of online payment systems for monthly bills. EBPP services allow consumers to view bills electronically and pay them through electronic funds transfers from bank or credit card accounts.
 - Major players in the EBPP marketplace include: online banking, biller-direct systems, mobile payment systems, and consolidators.

QUESTIONS

1. Why is it less risky to steal online? Explain some of the ways criminals deceive consumers and merchants.
2. Explain why an e-commerce site might not want to report being the target of cybercriminals.
3. Give an example of security breaches as they relate to each of the six dimensions of e-commerce security. For instance, what would be a privacy incident?
4. How would you protect your firm against a Denial of Service attack?
5. Name the major points of vulnerability in a typical online transaction.
6. How does spoofing threaten a website’s operations?
7. Why is adware or spyware considered to be a security threat?
8. What are some of the steps a company can take to curtail cybercriminal activity from within a business?
9. Explain some of the modern-day flaws associated with encryption. Why is encryption not as secure today as it was earlier in the century?
10. Briefly explain how public key cryptography works.
11. Compare and contrast firewalls and proxy servers and their security functions.
12. Is a computer with anti-virus software protected from viruses? Why or why not?
13. Identify and discuss the five steps in developing an e-commerce security plan.
14. How do biometric devices help improve security? What particular type of security breach do they reduce?
15. Briefly discuss the disadvantages of credit cards as the standard for online payments. How does requiring a credit card for payment discriminate against some consumers?
16. Describe the major steps involved in an online credit card transaction.
17. Why is Bitcoin so controversial?
18. What is NFC and how does it work?
19. Discuss why EBPP systems are becoming increasingly popular.
20. How are the main types of EBPP systems both alike and different from each other?

PROJECTS

1. Imagine you are the owner of an e-commerce website. What are some of the signs that your site has been hacked? Discuss the major types of attacks you could expect to experience and the resulting damage to your site. Prepare a brief summary presentation.
2. Given the shift toward m-commerce, do a search on m-commerce (or mobile commerce) crime. Identify and discuss the security threats this type of technology creates. Prepare a presentation outlining your vision of the new opportunities for cybercrime that m-commerce may provide.
3. Find three certification authorities and compare the features of each company's digital certificates. Provide a brief description of each company as well, including number of clients. Prepare a brief presentation of your findings.
4. Research the challenges associated with payments across international borders and prepare a brief presentation of your findings. Do most e-commerce companies conduct business internationally? How do they protect themselves from repudiation? How do exchange rates impact online purchases? What about shipping charges? Summarize by describing the differences between a U.S. customer and an international customer who each make a purchase from a U.S. e-commerce merchant.

REFERENCES

- Akamai Technologies, Inc. "Akamai's State of the Internet Q2 2016 Report." (September 2016).
- Akamai Technologies. "Exploitation of IoT devices for Launching Mass-Scale Attack Campaigns." (October 11, 2016b.)
- Alert Logic. "2015 Cloud Security Report." (2015).
- Arbor Networks. "Worldwide Infrastructure Security Report Volume XI." (2016).
- BI Intelligence. "Chase Adds Real-time P2P Payments." *Businessinsider.com* (June 15, 2016).
- Blue, Violet. "You Say Advertising, I Say Block That Malware." *Engadget.com* (January 8, 2016).
- Bureau of Consumer Financial Protection. "Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z)." [Docket No. CFPB-2014-0031] RIN 3170-AA22 (October 12, 2016).
- Center for Strategic and International Studies. "Net Losses: Estimating the Global Cost of Cybercrime." (June 2014).
- Chew, Hanley and Tyler G. Newby. "The Cybersecurity Information Sharing Act of 2015: An Overview." *Lexology.com* (October 24, 2016).
- Chirgwin, Richard. "Microsoft and FBI Storm Ramparts of Citadel Botnets." *The Register* (June 6, 2013).
- CIO.gov. "HTTP Strict Transport Security." (2016).
- Cisco. "2016 Cisco Annual Security Report." (2016).
- Cloud Security Alliance. "State of Cloud Security 2016." CSA Global Enterprise Advisory Board (2016).
- Constantin, Lucian. "Police Operation Disrupts Beebone Botnet Used for Malware Distribution." *Pcworld.com* (April 9, 2015).
- Cybersource, Inc. "Online Fraud Management Benchmarks: North American Edition." (2016).
- Cyphort. "Cyphort Labs Knocks Down the Top 8 Financial Malware." (October 15, 2015).
- Daly, Jim. "Report Documents the March of Online Alternatives to the Payments Mainstream." *Digital-transactions.net* (March 9, 2014).
- Datta, Saikat. "Security Breach in NIC Allowed Hackers to Issue Fake Digital Certificates—Hindustan Times." *Medianama.com* (August 14, 2014).
- Dell Inc. "Determining the True Costs of a Data Breach." (2015).
- Demos, Telis. "PayPal Gets Friendlier With Facebook." *Wall Street Journal* (October 24, 2016).
- DocuSign. "Going Mobile with Electronic Signatures." (2015).
- eMarketer, Inc. "Digital Payment Methods Used by US Internet Users, Aug 2016." (October 19, 2016a).
- eMarketer, Inc. "Mobile Wallet Adoption Among US Smartphone Users, by Provider, June 2016." (August 24, 2016b).
- eMarketer, Inc. (Rahul Chadha). "Global Ecommerce Platforms 2015: A Country-by-Country Look at the Top Retail Ecommerce Sites." (October 2015).
- Essers, Loek. "The 'Great Cannon' of China Enforces Censorship." *Computerworld.com* (April 10, 2015).

- Fiserv. "Eight Annual Billing Household Survey." (March 2016).
- Fiserv. "2007 Consumer Bill Payments Trends Survey: Volume of Electronic Payments." (2007).
- Fox, Emily Jane and Greg Botelho. "5 Charged in Credit Card Hacking Scheme Feds Call Largest Ever Prosecuted in the U.S." *Cnn.com* (July 25, 2013).
- Gartner. "Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach \$81.6 Billion in 2016." (August 16, 2016).
- Gemalto and Ponemon Institute. "Gemalto 2016 Global Cloud Data Security Study." (July 26, 2016).
- Goodin, Dan. "Big-Name Sites Hit by Rash of Malicious Ads Spreading Crypto Ransomware." *Arstechnica* (March 15, 2016).
- Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway—With Me In It." *Wired.com* (July 21, 2015).
- Hackett, Robert. "On Heartbleed's Anniversary, 3 of 4 Big Companies Are Still Vulnerable." *Fortune* (April 7, 2015).
- Hasham, Salim, Chris Rezek, Maxence Vancauwenbergh, and Josh Weiner. "Is Cybersecurity Incompatible with Digital Convenience?," *Mckinsey.com* (August 2016).
- Honan, Mat. "How Apple and Amazon Security Flaws Led to My Epic Hacking." *Wired.com* (August 6, 2012).
- IBM. "IBM Point of View: Internet of Things Security." (April 2015).
- Identity Theft Resource Center. "ITRC Data Breach Report." (January 25, 2016).
- Infosec Institute. "A Buyers Guide to Stolen Data on the Deep Web." *Darkmatters.norsecorp.com* (April 7, 2015).
- Internet Society. "Policy Brief: The Internet of Things." (October 7, 2016).
- Internet Society. "The Internet of Things: An Overview." (2015).
- Isaac, Mike. "WhatsApp Introduces End-to-End Encryption." *New York Times* (April 5, 2016).
- Javelin Strategy & Research. "2016 Identity Survey Report." (February 2, 2016).
- Johnson, N.F., M. Zheng, Y. Vorobyeva, A. Gabriel, H. Qi, N. Velasquez, P. Manrique, D. Johnson, E. Restrepo, C. Song, and S. Wuchty. "New Online Ecology of Adversarial Aggregates: ISIS and Beyond." *Science* (June 17, 2016).
- Keizer, Greg. "XcodeGhost Used Unprecedented Infection Strategy Against Apple." *Computerworld.com* (September 26, 2015).
- Kirk, Jeremy. "Zero Day, Web Browser Vulnerabilities Spike in 2014." *Networkworld.com* (March 25, 2015a).
- Korolov, Maria. "Most Corporate Risk Due to Just 1% of Employees." *Csoonline.com* (August 26, 2015).
- Leger, Donna Leinwand. "Credit Card Info Sold on Hacker Sites." *USA Today* (September 4, 2014).
- Leising, Matthew. "CME Teams Up with Dwolla to Bring Real-Time Payments to Exchange." *Bloomberg.com* (October 28, 2015).
- Loeb, Larry. "Malwarebytes Thinks Potentially Unwanted Programs Are Malware." *SecurityIntelligence.com* (October 13, 2016).
- Loten, Angus. "Cloud Security Fears Persist." *Wall Street Journal* (October 17, 2016).
- Majkowski, Marek. "Mobile Ad Networks as DDoS Vectors: A Case Study." *Blog.cloudflare.com* (September 25, 2015).
- Maruca, William. "Hacked Health Records Prized for their Black Market Value." *Hipaahealthlaw.foxrothchild.com* (March 16, 2015).
- McAfee. "The Hidden Data Economy: The Marketplace for Stolen Digital Information." (October 15, 2016).
- McMillan, Robert. "In the Bitcoin Era, Ransomware Attacks Surge." *Wall Street Journal* (August 19, 2016).
- Microsoft. "Microsoft Security Intelligence Report Volume 20: July–December 2015." (May 5, 2016).
- Mitnick, Kevin. *Ghost in the Wires*. Little, Brown & Co. (2011).
- Neustar. "April 2016 Neustar DDoS Attacks and Protection Report: North America & EMEA." (April 2016).
- Pagliery, Jose. "FBI Teams Up with Hackers to Bust Bank Robbing Botnet." *Cnn.com* (October 13, 2015).
- Panda Security. "PandaLabs' Annual Report 2015." (2016).
- Patane, Matthew. "Dwolla Drops Transaction Fees to Gain Ground." *Des Moines Register* (June 4, 2015).
- PCI Security Standards Council. "Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedure Version 3.1." (April 2015).
- Pendell, Ryan. "Why Dwolla Made Its Transactions Free (And What Happened Next)," *Siliconprairienews.com* (June 21, 2016).
- Perloth, Nicole. "Apple Will Pay a 'Bug Bounty' to Hackers Who Report Flaws." *New York Times* (August 4, 2016).
- Perloth, Nicole, and Vindu Goel. "Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say." *New York Times* (September 28, 2016).
- Peterson, Andrea. "Senate Passes Cybersecurity Information Sharing Bill Despite Privacy Fears." *Washington Post* (October 27, 2015).
- Ponemon Institute. "2015 Cost of Data Breach Study: United States." (June 2016a).
- Ponemon Institute. "2015 Cost of Cyber Crime Study: United States." (October 2015a).

- Ponemon Institute. "The Unintentional Insider Risk in the United States and German Organizations." (July 2015b).
- PWC. "US Cybersecurity: Progress Stalled. Key Findings from the 2015 US State of Cybercrime Survey." (June 2015).
- RAND Corporation. "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar." (2014).
- Sanger, David and Nicole Perlroth. "A New Era of Internet Attacks Powered by Everyday Devices." *New York Times* (October 22, 2016).
- Sidel, Robin. "Credit Card Scammers Flock to Online Shopping." *Wall Street Journal* (October 25, 2016).
- Schuman, Evan. "Starbucks Caught Storing Mobile Passwords in Clear Text." *Computerworld* (January 15, 2014).
- Schwartz, John. "Fighting Crime Online: Who Is in Harm's Way?" *New York Times* (February 8, 2001).
- Silanis Technology. "Security for E-Signatures and E-Transactions: What to Look for in a Vendor." (2014).
- Software Engineering Institute. "Common Sense Guide to Mitigating Insider Threats, 4th Edition." Sei.cmu.edu (December 2012).
- Stein, Lincoln D. *Web Security: A Step-by-Step Reference Guide*. Reading, MA: Addison-Wesley (1998).
- Storm, Darlene. "MEDJACK: Hackers Hijacking Medical Devices Create Backdoors in Hospital Networks." *Computerworld.com* (June 8, 2015a).
- Storm, Darlene. "2 More Wireless Baby Monitors Hacked: Hackers Remotely Spied on Babies and Parents." *Computerworld.com* (April 22, 2015b).
- Symantec, Inc. "Internet Security Threat Report 2016 Volume 21." (April 2016).
- Symantec, Inc. "Internet Security Threat Report 2015 Volume 20." (April 2015).
- U.S. Department of Justice. "How to Protect Your Networks From Ransomware." (2016).
- Vaughan-Nichols, Steven J. "FREAK: Another Day, Another Serious SSL Security Hole." *Zdnet.com* (March 3, 2015).
- Vaughan-Nichols, Steven J. "Has the NSA Broken SSL? TLS? AES?" *Zdnet.com* (September 6, 2013).
- Verizon. "2016 Data Breach Investigations Report." (2016).
- Vijayan, Jaikumar. "Google Joins Yahoo, AOL, in Adopting Stricter Email Authentication." *Eweek.com* (October 20, 2015).
- Voreacos, David. "5 Hackers Charged in Largest Data Breach Scheme in U.S." *Bloomberg.com* (July 26, 2013).
- Wakabayashi, Daisuke. "A Contrite Sony Vows Tighter Security." *Wall Street Journal* (May 1, 2011).
- Wills, Amanda. "New Snowden Leak: NSA Program Taps All You Do Online." *Mashable.com* (August 1, 2013).
- Wingfield, Nick. "Spam Network Shut Down." *Wall Street Journal* (March 18, 2011).
- Zarras, Apostolis, Alexander Kapravelos, Gianluca Stringhini, Thorsten Holz, Christopher Krugel, and Giovanni Vigna. "The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements." ICM '14 Vancouver, BC, Canada (November 5–7, 2014).



CHAPTER

11

Social Networks, Auctions, and Portals

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Describe the different types of social networks and online communities and their business models.
- Describe the major types of auctions, their benefits and costs, how they operate, when to use them, and the potential for auction abuse and fraud.
- Describe the major types of Internet portals and their business models.

Social Network Fever

Spreads to the Professions

When social networks first appeared a decade ago, it was widely believed the phenomenon would be limited to crazed teenagers already captive to online games and video game consoles. Most of the technorati in Silicon Valley and Wall Street felt this was a blip on the horizon, and their full attention was occupied by search engines, search engine marketing, and ad placement. But when the population of social network participants pushed into the hundreds of millions, even the technical elite woke up to the fact that these huge audiences were not just a bunch of teenagers. Instead, a wide slice of American society was participating. Steve Ballmer, Microsoft's CEO at the time, expressed the conviction as early as 2007 that social networks would have some staying power, although he tempered that outlook with reservations about just how long that would be, given their youthful appeal and faddish nature. This was just before Microsoft paid \$250 million for a small stake in Facebook, which valued the company at \$15 billion. Trying to sound convincing, the month before his company spent \$1.65 billion for YouTube, Google CEO Eric Schmidt asserted his belief that despite prevailing opinion, social networks were a bona fide business opportunity.

Today, the social network craze has taken a firm hold. In addition to the hugely popular social networks aimed at the general population, such as Facebook, which now has over 1.7 billion active monthly users worldwide, there are a number of social networks aimed at more specific groups. Take LinkedIn, for example, probably the best-known and most popular business network site. LinkedIn has more than 450 million members in over 200 countries, representing 170 different industries. In 2016, according to LinkedIn, it typically has around 110 million monthly unique visiting members, including about 60 million who visit using a mobile device. In May 2011, LinkedIn went public in what was, at the time, the biggest Internet IPO since Google, raising more than \$350 million and giving it a company valuation of \$8.9 billion. In 2016, Microsoft acquired LinkedIn for a whopping \$26.2 billion. Although the price tag gave many analysts pause, the acquisition is a logical fit, giving Microsoft a long-desired social media presence as well as a tool to promote its Microsoft Office programs to professional audiences. LinkedIn's stock price rebounded from 3-year lows in the wake of the news, and reached \$192 per share in September 2016. LinkedIn allows a member to create a profile, including a photo, to summarize his or her professional accomplishments. Members' networks include their connections, their connections' connections, as well as people they know, potentially linking them to thousands of others. How members use LinkedIn depends somewhat on their



Courtesy of Carol Traver

SOURCES: "About Us," LinkedIn.com Press Center, accessed October 5, 2016; "LinkedIn Unveils Its New Blogging Platform," by Eileen Brown, Zdnet.com, September 8, 2016; "Professional 'Gold Mine' Or 'Cheesy' Irritant? Why We Love (And Hate) LinkedIn," by Kevyn Burger, Startribune.com, September 3, 2016; "LinkedIn Just Joined the 'Gig Economy.' Here's How," by John Nemo, Inc.com, August 24, 2016; "Why Microsoft Bought LinkedIn," by Christopher Mims, *Wall Street Journal*, June 14, 2016; "Microsoft to Acquire LinkedIn for \$26.2 Billion," by Jay Greene, *Wall Street Journal*, June 14, 2016; "Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent Over the Last Decade," Careerbuilder.com, April 28, 2016; LinkedIn Form 10K for the fiscal year ending December 31, 2015, filed with the U.S. Securities and Exchange Commission, February 4, 2016; "Welcome to The CAPS Community," Caps.fool.com, accessed October 21, 2015; "New Social Network Aims to Find News Tech Pros Really Care About," by Kristin Burnham, Computerworld.com, September 21, 2015; "35 Percent of Employers Less Likely to Interview Applicants They Can't Find Online, According to Annual CareerBuilder Social Media Recruitment Survey," Careerbuilder.com, May 14, 2015.

position. Top executives use the site to promote their businesses, while job seekers use the site to find a new position. Firms looking for new hires use the site as an important source of professional talent. LinkedIn hopes that its more influential users will make use of its retooled LinkedIn Publishing blogging platform to connect with audiences. And in response to the increase in freelance jobs and growth in the "gig economy," LinkedIn unveiled its ProFinder marketplace in 2016, which allows consumers to find independent service providers for part-time or temporary jobs.

Those with a particular interest in the stock market can choose from a crop of financial social networks that allow users to connect with other investors, discuss issues focused on the stock market, and sometimes just show off investing prowess. For example, Stockr is a community where stock investors exchange ideas and track the performance of financial bloggers. The Motley Fool, one of the best-known online stock investment services, started its CAPS stock-rating social network in 2006 and now has over 180,000 members.

You can find similar social networks for a variety of specific professional groups such as health care (DailyStrength), law (LawLink), physicians (Sermo), human resources (Hr.com), and Quibb (technology professionals). These social networks encourage members to discuss the realities of their professions and practices, sharing successes and failures. The rapid growth of professional social networks, linked to industry and careers, demonstrates how widespread and nearly universal the appeal of social networks is. What explains the very broad attraction to social networks? E-mail is excellent for communicating with other individuals, or even a small group. But e-mail is not very good at getting a sense of what others in the group are thinking, especially if the group numbers more than a dozen people. The strength of social networks lies in their ability to reveal group attitudes and opinions, values, and practices.

Professionals who join social networks need to be careful about the content they provide, and the distribution of this content. As business social networks have grown, and as the number of participants expands, employers are finding them a great place to discover the "inner" person who applies for a job. A 2016 survey by CareerBuilder, the most widely used employment site in the United States, found that 60% of employers use social networks to screen job candidates, a large increase from 52% in 2015 and a far cry from the 11% recorded in 2006. The survey found that 49% of hiring managers who use social media to vet candidates discovered information that led them not to hire an applicant, such as provocative material posted by the candidate, information about the candidate drinking or using drugs, or criticism by the candidate of former employers. On the other hand, 32% of managers found information that led them to hire someone, such as evidence of a professional image, well-rounded personality, creativity, and good communication skills. Based on this survey, it's wise to use social networks' maximum privacy settings and release to the public only the most innocuous content. Likewise, be cautious of social networks that do not provide "take down" policies, which allow users to remove embarrassing materials from their pages.

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 marketplace, in some countries, localized social networks are significant, 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?

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

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

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.

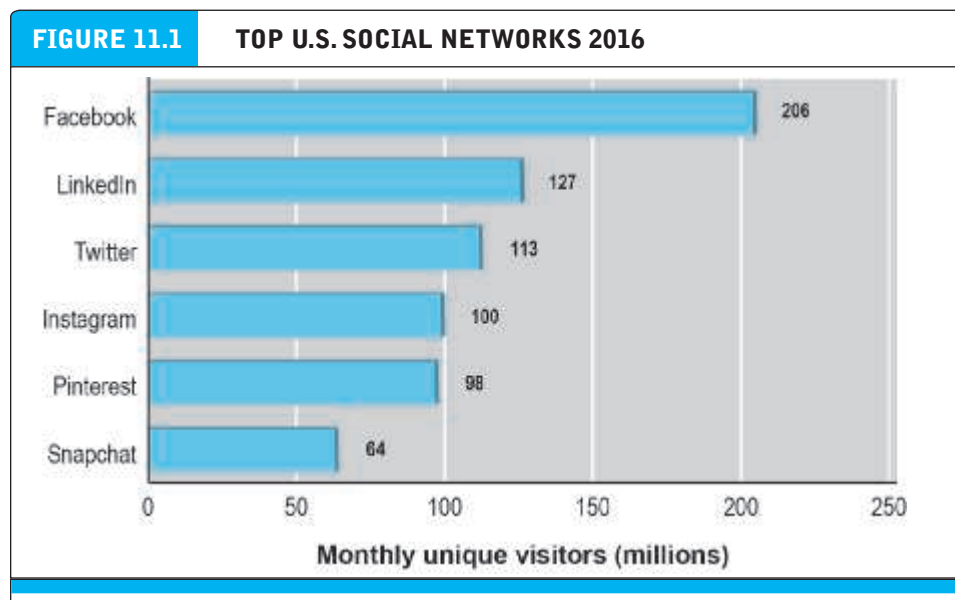
It's a short step to defining an **online social network** as an online location where people who share common ties can interact with one another. This definition is very close to that of Howard Rheingold's—one of The Well's early participants—who coined the term *virtual communities* as “cultural aggregations 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.



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.

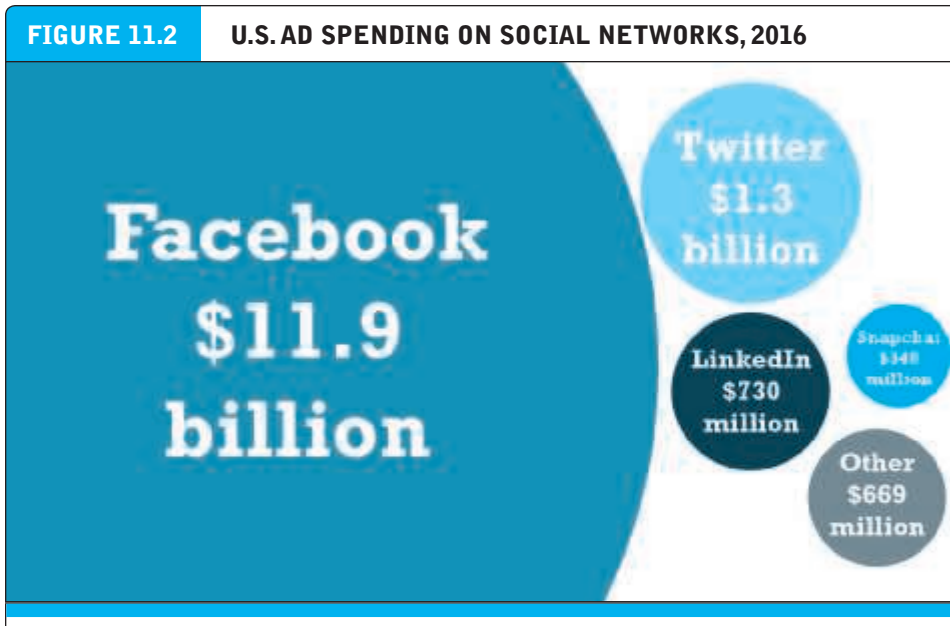
the United States in 2016 are expected to generate about \$15.4 billion in advertising revenue. Social networks are the fastest growing form of Internet usage and advertising revenue, but they are not yet as lucrative as traditional search engines/portals in terms of ad dollars generated. A part of the 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



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. 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-

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

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 pre-

sented 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," Nslc.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

affinity communities

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

sponsored communities

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

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

affinity groups

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

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” 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 are online communities created by government, non-profit, 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.

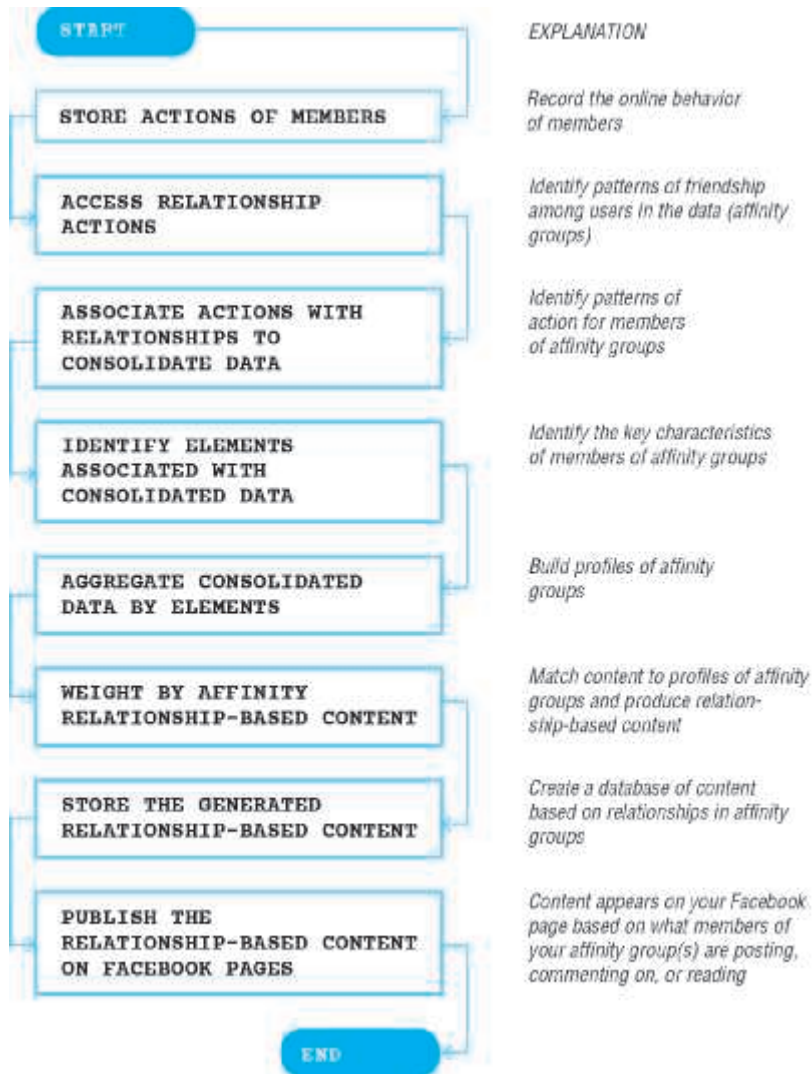
SOCIAL NETWORK TECHNOLOGIES AND FEATURES

Algorithms 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

FIGURE 11.3

FACEBOOK'S ALGORITHM FOR GENERATING PERSONALIZED STORIES



Facebook uses a very complex algorithm to identify content that users are likely to click on. Each step in the algorithm is implanted by computer programs involving tens of thousands of lines of computer code and thousands of hours of software engineering and system development.

SOURCE: Based on data from U.S. Patent and Trademark Office, 2010.

are, as well as demographic and other personal information. Once these are identified, Facebook attempts to find out what content is being consumed by each affinity group and matches the content to each group (relation-base content). Facebook creates a database of this relationship-based content, and serves it to other members of the group, as well as other affinity groups that share similar features.

In the end, you will be informed of what your friends are doing, liking, viewing and listening to. You will find this interesting and engaging. You will be spared hearing about other affinity groups who are very dissimilar to your affinity groups. New content (news, music, videos) that is similar to what your affinity group has liked in the past will also be served to you. For instance, if you are a staunch conservative or liberal, and you choose to click on articles that confirm your views, other members of your affinity group who share your views will have the content and your behavior displayed on their pages. They in turn may share this content with other Facebook friends, and other affinity groups of which they are a part.

While the generic algorithm appears simple, each step in the algorithm is implemented by computer programs involving tens of thousands of lines of computer code, and thousands of hours of software engineering and system development. The data produced by over 167 million users in the United States, and 1.7 billion other users worldwide requires three data centers in the United States and one in Sweden, a total of a million square feet containing tens of thousands of servers, all connected by several fiber optic networks (Data Center Knowledge, 2016). According to Facebook, loading a user's home page involves hundreds of servers, processing tens of thousands of individual pieces of data, and delivering the information selected in less than one second. The *Insight on Technology* case, *Trapped Inside the Facebook Bubble?*, examines the impact of algorithms in further depth.

Social networks also have developed a number of other software applications that allow users to engage in a number of activities. **Table 11.4** describes several additional social network functionalities.

TABLE 11.4 SOCIAL NETWORK FEATURES	
FEATURE	DESCRIPTION
Profiles	User-created web pages that describe the owner on a variety of dimensions
Newsfeed	A listing of updates from friends, advertisements, and notifications in chronological order
Timeline	A history of updates, posts from friends, photos, and other objects in chronological order
Friends networks	Ability to create a linked group of friends, a social community
Network discovery	Ability to find other social networks, find new groups and friends, and discover friends of friends
Favorites (Like)	Ability to communicate favorite sites, bookmarks, content, and destinations
Games and apps	Games developed for the social network, and apps that extend its functionality
Instant messaging	Instant messaging, chat
Storage	Storage for photos, videos, text
Message boards	Ability to post updates to friends, e.g., Wall
Groups	Discussion groups, forums, and consumer groups organized by interest, e.g., For Sale Groups

INSIGHT ON TECHNOLOGY

TRAPPED INSIDE THE FACEBOOK BUBBLE?



In May 2016, the blog Gizmodo published a report claiming that Facebook suppressed conservative political stories in its Trending section by allowing its news curators to intervene in the operation of Facebook's Trending algorithm, which allegedly chose trending topics based organically on Facebook's users' likes, mentions, posts, and clicks. There was, so the article claimed, a liberal bias at Facebook. The article, based on claims of former employees, led to a flurry of critical news articles, a potential Congressional investigation, a public debate over Facebook's role in promoting its own political agenda, and a great deal of commentary about the role of Facebook in shaping the news that Americans read everyday.

A related debate arose concerning the role of Facebook's entire News Feed algorithm, which displays posts by your Facebook friends, as well as ads based in part on Facebook's knowledge of you and your friends. Critics fear that both the News Feed and Trending section are helping to create a highly polarized society: users see only the social and political views of their friends on controversial topics, creating a self-reinforcing, bubble world. Sometimes referred to as the Facebook filter trap, echo chamber, or bubble, critics believe this results in groups who never share news or interact with one another, and who therefore cannot find a middle ground to share. Worse, extremist groups proliferate based on their own unchallenged facts and theories, which are never subjected to accuracy checking. It's called homophily: given a choice, people tend to associate with people like themselves. In the social network world, this translates to only being exposed to views of people who share your views, creating an echo chamber. Contrary views will rarely make it to your News Feed or your Trending feed. Every click, every Like, and

keystroke creates a reality for users that may or may not be a fiction.

From Facebook's point of view, both the News Feed and Trending algorithms solve an important problem for today's users of social networks: there is so much information online that users may become inundated with information that does not interest them, and makes it difficult for them to find information that does interest them. The resulting frustration could turn users away from social networks that increasingly are the source of news and opinion for web users. Therefore there is a need for what Facebook refers to, in its patent applications for both algorithms, as "a system to generate dynamic, relationship-based content personalized for members of a Social Network." Translated, this means the algorithms are set up to engage you and keep you on the site, exposing you to more ads.

The Trending algorithm is a complex chunk of code that operates in real time. The algorithm monitors the behavior of over 200 million users in the United States and over 1 billion worldwide, and posts the results on the top right of users' News Feed pages, changing periodically through the day. The algorithm is also sensitive to rates of change: if mentions spike in a short period of time, the topic gets boosted in ranking. Facebook certainly gave users the impression that Trending was a computer-driven process that accurately and objectively reflects what other users were reacting to on the social network and what you are likely to click on.

But the reality was really quite different, according to Gizmodo and former employees. The process of selecting trends evolved over several years, but from the beginning news curators (journalists) intervened and had the last say about what was, or was not, included in Trending. As it turns out, the algorithm could not distinguish between a



real event (a SpaceX rocket exploded on the pad) versus a phony event (spacemen land in New Mexico), or if a topic was covered elsewhere as a live topic on Facebook. The algorithm was not allowed to include stories about Facebook itself. If the algorithm missed important news events for some reason, curators injected these events and views as Trending topics. Often, with complex algorithms, how they produce results is not precisely understood even by their authors, and the results of the algorithm may not quite hit the mark. Hot topics identified by the algorithm that involved sex, pornography, nudity, graphic violence, or “R” rated content were removed by editors. Humans played an important editorial role in creating the Trending topics, and like journalists and editors everywhere, could exercise their discretion and perhaps insert their political views, in the process. In many ways, this sounds just like an ordinary newspaper or television news program: selecting news that editors think will be of interest to its readership, using headlines, lists, and sidebars to other stories.

An examination of Facebook’s patent describing the Trending algorithm reveals that a variety of other factors are used to create the Trending list. The algorithm uses keywords to process mentions and other activities of users (such as Super Bowl, skiing, baseball, etc.) and groups them into topics. Each topic is given a trending score based on the geographic location of users posting about the topic, the number of mentions, and the rate of increase in activity. Then the trending topics are matched to the personal interests of your friends on the social network, and of each user, as well as other factors like gender, race, national origin, religion, age, marital status, disability, sexual orientation, educational level, and socioeconomic statuses. In short, just about everything you have ever shared with Facebook!

The net result is that the Trending topics you see are likely different from those displayed to your next-door neighbor, friends who live in a different

state, colleagues at work, or millions of others who see their own personalized topics. The Trending topics do not reflect the Facebook user audience, but instead are Facebook’s best estimate of what you would find engaging, what your friends have found engaging, and what you are more likely to click on, thereby keeping you on Facebook for the display of ads. Facebook is in the business of manufacturing advertising revenues through increasing engagement, i.e., time on site. Facebook is not a news organization in the traditional sense, but a redistributor of content created by others, whether professional journalists or amateur bloggers.

One of the vulnerabilities of the Trending algorithm is its sensitivity to the number of mentions (which could be Likes, posts, clicks, or other behavior), and the rate of increase over short periods of time. Social scientists established a long time ago that on most controversial issues, 90% of the population appears near the middle of opinion, or close by. The other 10% of the population has views that are significantly further away from the average opinion. Sometimes called “fringe groups” or “extremists,” people in these groups often are highly engaged, very active contributors to Facebook and other opinion sites, often espouse conspiracy theories, engage in hate speech, and do so in a concerted short-term burst of online posting in the hope of influencing a very large online audience by encouraging a viral sharing of their posts. Fringe groups try to take advantage of the viral nature of social networks. Facebook’s algorithm tries to counter this tendency by demoting content posted by very frequent contributors.

In response to the public concern about liberal bias in the Trending section, and the difficulty Facebook encountered in trying to clearly explain how its Trending section works, Facebook fired its staff of 26 Trending editors in 2016, and promised to rely only on the Trending algorithm in order to eliminate human bias and be more objective. The early results suggest that more false news stories, conspiracy theories, and offensive material are appearing in

Trending than before. As one pundit noted, with its human editors dismissed, Facebook has let the inmates—Facebook users—run the asylum.

The News Feed also faces similar criticism. To illustrate the strength of the News Feed echo chamber, and how reality differs for different Facebook users, the *Wall Street Journal* publishes a graphical representation of how very liberal and very conservative users of Facebook linked to (reacted to) news articles drawn from over 500 sources, from bloggers to reputable news organizations. The data was originally produced in a large study of user behavior funded by Facebook, conducted by Facebook researchers, and reported in the magazine *Science*. The News Feeds of 10 million users were examined. The results of the *Journal's* online data is that very liberal and very conservative Facebook users create for themselves, through their selection of news articles enabled by the News Feed algorithm, two highly divergent world views on most topics, from guns, to abortion, ISIS, political candidates, and so forth. For instance, on guns, very liberal users linked to news posts critical of the National Rifle Association, school shootings, and the ready availability of guns, among others. Very conservative users linked to news posts critical of gun control legislation, invasions of homes by armed criminals, and the use of guns for self-defense, among others. Facebook's researchers concluded in the *Science* article that Facebook's users do get some contrary views in their News Feeds and Trend-

ing sections, and that any bias is not caused by its algorithms, but rather by users selecting as friends people who share their views. The algorithms simply reflect what users have chosen in terms of friends and the articles they click on.

If you want to know why liberals and conservatives have a difficult time communicating with one another, let alone acting on key issues together, it's because they reside in two very different, polarized news streams. Since well over half of the online population gets its news from social networks like Facebook, what Facebook determines is news has a significant impact on public debate and policy.

On the other hand, is Facebook any different from a traditional newspaper or cable news channel, both of which select the news and views that they believe their readers and viewers find engaging? One difference is that for traditional news producers, human beings are doing the selection of news, and viewers understand this, and select among the offerings. At Facebook, algorithms, written by humans, automate this process of determining what is news.

The algorithms of Trending cannot discern the validity of articles, the difference between a crackpot conspiracy theory, and a quality piece of well-researched journalism. Those who join any community on Facebook are algorithmically driven to receive more and more content supported by that group, and less content from opposing groups or views.

SOURCES: "Blue Feed, Red Feed: See Liberal Facebook and Conservative Facebook, Side by Side," *Wall Street Journal*, May 18, 2016; "The Algorithm Is an Editor," by Jeffrey Herbst, *Wall Street Journal*, April 13, 2016; "Facebook's 'Trending' Feature Exhibits Flaws Under New Algorithm," by Georgia Wells, *Wall Street Journal*, September 6, 2016; "Almost No One Really Knows How Facebook's Trending Algorithm Works, But Here's An Idea," by Joseph Lichterman, NiemanLab.org, September 1, 2016; "Inside Facebook's (Totally Insane, Unintentionally Gigantic, Hyperpartisan) Political-Media Machine," by John Herrman, *New York Times*, August 24, 2016; "The Reason Your Feed Became An Echo Chamber—And What To Do About It," NPR.com, July 24, 2016; "Your Facebook Echo Chamber Just Got a Whole Lot Louder," by Brian Barrett, *Wired.com*, June 29, 2016; "Exposure to Ideologically Diverse News and Opinion on Facebook," by E. Bakshy, S. Messing, and L. Adamic, *Science*, June 5, 2016; "How Facebook Warps Our Worlds," by Frank Bruni, *New York Times*, May 21, 2016; "The Wall Street Journal's New Tool Gives a Side-by-Side Look at the Facebook Political News Filter Bubble," by Ricardo Bilton, *Wall Street Journal*, May 18, 2016; "Facebook Study Finds People Only Click on Links That They Agree With, Site Is an 'Echo Chamber'," by Andrew Griffin, *Independent.co.uk*, May 8, 2015; *The Filter Bubble*, by Eli Pariser. Penguin Books; Reprint edition (April 24, 2012); Facebook, "Generating a Feed of Stories Personalized For Members of a Social Network," US Patent 7827208 B2, United States Patent Office, published November 2, 2010.

What is the difference between C2C and a B2C auctions?

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

business-to-consumer (B2C) auctions

business sells goods it owns, or controls, using various dynamic pricing models

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.

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

popularity, or occurrence.

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.

1

Benefits of Auctions

List and briefly explain four of the benefits of auction markets?

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.

- 2 • **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.
- 3 • **Price transparency:** Public Internet auctions allow everyone in the world to see the asking and bidding prices for items.
- 4 • **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.
- 5 • **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.
- 6 • **Consumer aggregation:** Sellers benefit from large auction sites' ability to aggregate a large number of consumers who are motivated to purchase something in one marketplace.

- 7 • **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

What are the four major costs to consumers of participating in an auction?

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:

- 1 • **Delayed consumption costs:** Internet auctions can go on for days, and shipping will take additional time.
- 2 • **Monitoring costs:** Participation in auctions requires your time to monitor bidding.
- 3 • **Equipment costs:** Internet auctions require you to purchase a computer system and pay for Internet access.
- Risk • **Trust risks:** Online auctions are a significant source of Internet fraud. Using auctions increases the risk of experiencing a loss. التعرض للخسارة
- 4 requirement • **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

list and describe four different types 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.

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.

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).

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

English auction

most common form of auction; the highest bidder wins

1

Dutch Internet auction

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

2

Name Your Own Price auction

auction where users specify what they are willing to pay for goods or services

3

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.

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.

penny (bidding fee) auction

bidder must pay a non-refundable fee to purchase bids

4

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

TABLE 11.6

FACTORS TO CONSIDER WHEN CHOOSING AUCTIONS

CONSIDERATIONS	DESCRIPTION
Type of product	Rare, unique, commodity, perishable
Stage of product life cycle	Early, mature, late
Channel-management issues	Conflict with retail distributors; differentiation
Type of auction	Seller vs. buyer bias
Initial pricing	Low vs. high
Bid increment amounts	Low vs. high
Auction length	Short vs. long
Number of items	Single vs. multiple
Price-allocation rule	Uniform vs. discriminatory
Information sharing	Closed vs. open bidding

market for the goods. However, Priceline has succeeded in developing auctions for perishable commodities (such as airline seats) for which retail prices have already been established, and some B2B auctions involve commodities such as steel (often sold at distress prices). New clothing items, new digital cameras, and new computers are generally not sold at auction because their prices are easy to discover, catalog prices are high, sustainable, and profitable, they are not perishable, and there exists an efficient market channel in the form of retail stores (online and offline).

- **Product life cycle:** For the most part, businesses have traditionally used auctions for goods at the end of their product life cycle and for products where auctions yield a higher price than fixed-price liquidation sales. However, products at the beginning of their life cycle are increasingly being sold at auction. Early releases of music, books, videos, games, and digital appliances can be sold to highly motivated early adopters who want to be the first in their neighborhood with new products. Online auctions and sales of event tickets from music concerts to sports events now account for more than 50% of all event ticket sales in the United States.
- **Channel management:** Established retailers such as JCPenney and Walmart, and manufacturers in general, must be careful not to allow their auction activity to interfere with their existing profitable channels. For this reason, items found on established retail-site auctions tend to be late in their product life cycle or have quantity purchase requirements.
- **Type of auction:** Sellers obviously should choose auctions where there are many buyers and only a few, or even one, seller. English ascending-price auctions such as those at eBay are best for sellers because as the number of bidders increases, the price tends to move higher.
- **Initial pricing:** Research suggests that auction items should start out with low initial bid prices in order to encourage more bidders to bid (see “Bid increments” below).

The lower the price, the larger the number of bidders will appear. The larger the number of bidders, the higher the prices move.

- **Bid increments:** It is generally safest to keep bid increments low so as to increase the number of bidders and the frequency of their bids. If bidders can be convinced that, for just a few more dollars, they can win the auction, then they will tend to make the higher bid and forget about the total amount they are bidding.
- **Auction length:** In general, the longer auctions are scheduled, the larger the number of bidders and the higher the prices can go. However, once the new bid arrival rate drops off and approaches zero, bid prices stabilize. Most eBay auctions are scheduled for seven days.
- **Number of items:** When a business has a number of items to sell, buyers usually expect a “volume discount,” and this expectation can cause lower bids in return. Therefore, sellers should consider breaking up very large bundles into smaller bundles auctioned at different times.
- **Price allocation rule:** Most buyers believe it is “fair” that everyone pay the same price in a multi-unit auction, and a uniform pricing rule is recommended. eBay Dutch Internet auctions encourage this expectation. The idea that some buyers should pay more based on their differential need for the product is not widely supported. Therefore, sellers who want to price discriminate should do so by holding auctions for the same goods on different auction markets, or at different times, to prevent direct price comparison.
- **Closed vs. open bidding:** Closed bidding has many advantages for the seller, and sellers should use this approach whenever possible because it permits price discrimination without offending buyers. However, open bidding carries the advantage of “herd effects” and “winning effects” (described later in the chapter) in which consumers’ competitive instincts to “win” drive prices higher than even secret bidding would achieve.

AUCTION PRICES: ARE THEY THE LOWEST?

It is widely assumed that auction prices are lower than prices in other fixed-price markets. Empirical evidence is mixed on this assumption. There are many reasons why auction prices might be higher than those in fixed-price markets for items of identical quality, and why auction prices in one auction market may be higher than those in other auction markets. Consumers are not driven solely by value maximization but instead are influenced by many situational factors, irrelevant and wrong information, and misperceptions when they make market decisions (Simonson and Tversky, 1992). Auctions are social events—shared social environments, in which bidders adjust to one another (Hanson and Putler, 1996). Briefly, bidders base their bids on what others have previously bid, and this can lead to an upward cascading effect (Arkes and Hutzler, 2000). In a study of hundreds of eBay auctions for Sony PlayStations, CD players, Mexican pottery, and Italian silk ties, Dholakia and Soltysinski (2001) found that bidders exhibited herd behavior (the tendency to gravitate toward, and bid for, auction listings with one or more existing bids) by making multiple bids on some auctions (coveted comparables), and making no bids at auctions

What is herd behaviour and how does it impact auction?

herd behavior

the tendency to gravitate toward, and bid for, auction listings with one or more existing bids

attracted to something

desirable

ignore

for comparable items (overlooked comparables). Herd behavior resulted in consumers paying higher prices than necessary for reasons having no foundation in economic reality (Liu and Sutanto, 2012).

The behavioral reality of participating in auctions can produce many unintended results. Winners can suffer **winner's regret**, the feeling after winning an auction that they paid too much for an item, which indicates that their winning bid does not reflect what they thought the item was worth but rather what the second bidder thought the item was worth. Sellers can experience **seller's lament**, reflecting the fact that they sold an item at a price just above the second place bidder, never knowing how much the ultimate winner might have paid or the true value to the final winner. Auction losers can experience **loser's lament**, the feeling of having been too cheap in bidding and failing to win. In summary, auctions can lead to both winners paying too much and sellers receiving too little. Both of these outcomes can be minimized when sellers and buyers have a very clear understanding of the prices for items in a variety of different online and offline markets.

CONSUMER TRUST IN AUCTIONS

Auction sites have the same difficulties creating a sense of consumer trust as all other e-commerce sites, although in the case of auction sites, the operators of the marketplace do not directly control the quality of goods being offered and cannot directly vouch for the integrity of the buyers or the sellers. This opens the possibility for criminal or unreliable actors to appear as either sellers or buyers. Several studies have found that trust and credibility increase as users gain more experience, if trusted third-party seals are present, and if the site has a wide variety of consumer services for tracking purchases (or fraud), thus giving the user a sense of control (Krishnamurthy, 2001; Stanford-Makovsky, 2002; Nikander and Karvonen, 2002; Bailey et al., 2002; Kollock, 1999). Because of the powerful role that trust plays in online consumer behavior, eBay and most auction sites make considerable efforts to develop automated trust-enhancing mechanisms such as seller and buyer ratings, escrow services, buyer and seller insurance, guaranteed money back features, and authenticity guarantees (see the next section).

Name and describe five types of possible abuses and fraud that may occur with auctions?

winner's regret

the winner's feeling after an auction that he or she paid too much for an item

seller's lament

concern that one will never know how much the ultimate winner might have paid, or the true value to the final winner

loser's lament

the feeling of having been too cheap in bidding and failing to win

WHEN AUCTION MARKETS FAIL: FRAUD AND ABUSE IN AUCTIONS

Online and offline auction markets can be prone to fraud, which produces information asymmetries between sellers and buyers and among buyers, which in turn causes auction markets to fail. Some of the possible abuses and frauds include:

fraud

- **Bid rigging:** Agreeing offline to limit bids or using shills to submit false bids that drive prices up.
- **Price matching:** Agreeing informally or formally to set floor prices on auction items below which sellers will not sell in open markets.
- **Shill feedback, defensive:** Using secondary IDs or other auction members to inflate seller ratings.
- **Shill feedback, offensive:** Using secondary IDs or other auction members to deflate ratings for another user (feedback bombs).

الابتزاز

- **Feedback extortion:** Threatening negative feedback in return for a benefit.
- **Transaction interference:** E-mailing buyers to warn them away from a seller.
- **Bid manipulation:** Using the retraction option to make high bids, discovering the maximum bid of the current high bidder, and then retracting the bid.
- **Non-payment after winning:** Blocking legitimate buyers by bidding high, then not paying.
- **Shill bidding:** Using secondary user IDs or other auction members to artificially raise the price of an item.
- **Transaction non-performance:** Accepting payment and failing to deliver.
- **Non-selling seller:** Refusing payment or failing to deliver after a successful auction.
- **Bid siphoning:** E-mailing another seller's bidders and offering the same product for less.

Auction sites have sought to reduce these risks through various methods including:

- **Rating systems:** Previous customers rate sellers based on their experience with them and post them on the site for other buyers to see.
- **Watch lists:** These allow buyers to monitor specific auctions as they proceed over a number of days and only pay close attention in the last few minutes of bidding.
- **Proxy bidding:** Buyers can enter a maximum price they are willing to pay, and the auction software will automatically place incremental bids as their original bid is surpassed.

eBay and many other auction sites have investigation units that receive complaints from consumers and investigate reported abuses. Nevertheless, with millions of visitors per week and hundreds of thousands of auctions to monitor, eBay is highly dependent on the good faith of sellers and consumers to follow the rules.

11.3 E-COMMERCE PORTALS

Port: From the Latin *porta*, an entrance or gateway to a locality.

Portals are among the most frequently visited sites on the Web if only because they often are the homepage page to which many users point their browser on startup. The top portals such as Yahoo, MSN, and AOL have hundreds of millions of unique visitors worldwide each month. Portal sites are gateways to the billions of web pages available on the Internet. Facebook also acts as a home page portal to the Web. Millions of users have set Facebook as their home page, choosing to start their sessions with news from their friends, and many stay on Facebook for several hours a day. We have already discussed Facebook in Section 11.1. Perhaps the most important service provided by portals is to help people find the information they are looking for on the Web and, like newspapers, to expose people to information they were not looking for but which they nonetheless may find entertaining or interesting. The original portals in the early days of e-commerce were search engines. Consumers would pass through search engine portals on their way to rich, detailed, in-depth content on the Web. But portals evolved

into much more complex websites that provide news, entertainment, maps, images, social networks, in-depth information, and education on a growing variety of topics all contained at the portal site. Portals today seek to be a sticky destination site, not merely a gateway through which visitors pass. In this respect, portals are very much like television networks: destination sites for content supported by advertising revenues. Portals today want visitors to stay a long time—the longer the better to expose visitors to ads. For the most part they succeed: portals are places where people linger for a long time.

Portals also serve important functions within a business or organization. Most corporations, universities, churches, and other formal organizations have **enterprise portals that help employees or members navigate to important content, such as human resources information, corporate news, or organizational announcements.** For instance, your university has a portal through which you can register for courses, find classroom assignments, and perform a host of other important student activities. Increasingly, these enterprise portals also provide general-purpose news and real-time financial feeds provided by content providers outside the organization. Corporate portals and intranets are the subject of other textbooks focused on the corporate uses of web technology and are beyond the scope of this book (see Laudon and Laudon, 2016). Our focus here is on e-commerce portals.

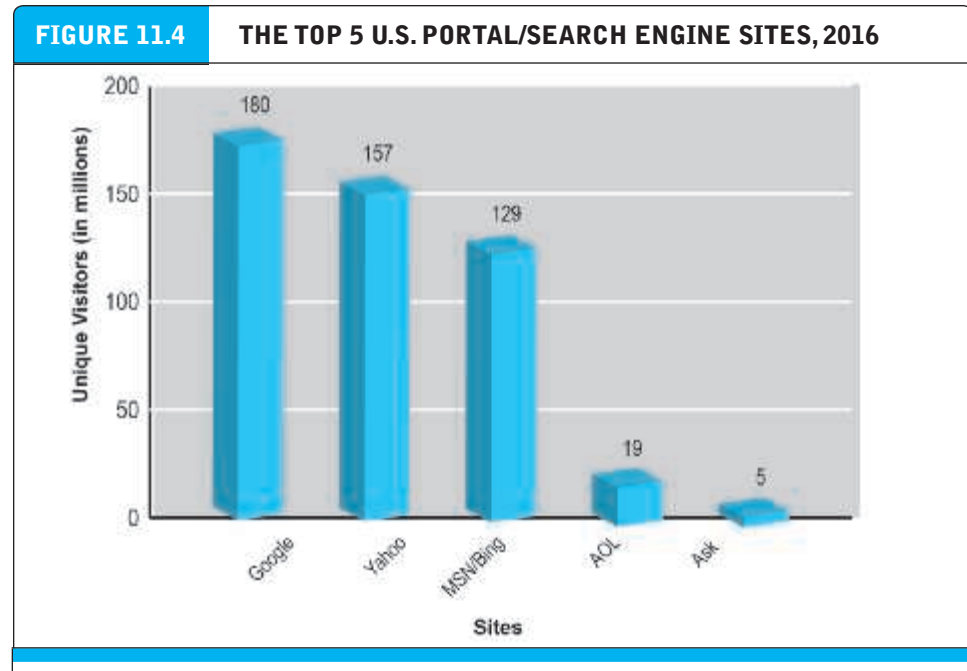
enterprise portals

help employees navigate to the enterprise's human resource and corporate content

THE GROWTH AND EVOLUTION OF PORTALS

Portals have changed a great deal from their initial function and role. As noted above, most of today's well-known portals, such as Yahoo, MSN, and AOL, began as search engines. The initial function provided by portals was to index web page content and make this content available to users in a convenient form. Early portals expected visitors to stay only a few minutes at the site. As millions of people signed on to the Internet in the early 2000s, the number of visitors to basic search engine sites exploded commensurately. At first, few people understood how a web search site could make money by passing customers on to other destinations. But search sites attracted huge audiences, and therein lay the foundation for their success as vehicles for marketing and advertising. Search sites, recognizing the potential for commerce, expanded their offerings from simple navigation to include commerce (the sale of items directly from the website as well as advertising for other retail sites), content (in the form of news at first, and later in the form of weather, investments, games, health, and other subject matter), communications (email, chat, and texting), and distribution of others' content. These four characteristics have become the basic definition of portal sites, namely, sites that provide four functions: navigation of the Web (search), communications, commerce, and content.

Because the value of portals to advertisers and content owners is largely a function of the size of the audience each portal reaches, and the length of time visitors stay on site, portals compete with one another on reach and unique visitors. *Reach* is defined as the percentage of the web audience that visits the site in a month (or some other time period), and *unique visitors* is defined as the number of uniquely identified individuals who visit in a month. Portals are inevitably subject to network effects: The value of the portal to advertisers and consumers increases geometrically as reach increases, which, in turn, attracts still more customers. These effects have resulted in the differentiation of the portal marketplace into three tiers: a few general-purpose mega



SOURCE: Based on data from Compete.com, 2016.

portal sites that garner 60%–80% of the web audience, second-tier general-purpose sites that hover around 20%–30% reach, and third-tier specialized vertical market portals that attract 2%–10% of the audience. As described in Chapter 3, the top five portals/search engines (Google, Yahoo, MSN/Bing, AOL, and Ask) account for more than 95% of online searches. A similar pattern of concentration is observed when considering the audience share of portals/search engines (including both desktop and mobile) as illustrated in **Figure 11.4**. However, this picture is changing as large audiences move to social network sites, and millions of users make these sites their opening or home pages and the place where they spend most of their digital time. Social network sites like Facebook are broadening their content with videos, movies, and news, transforming themselves into a hybrid social network and portal.

For more insight into the nature of the competition and change among the top portals, read *Insight on Business: Verizon Doubles Down on Portals*.

TYPES OF PORTALS: GENERAL-PURPOSE AND VERTICAL MARKET

There are two primary types of portals: **general-purpose portals** and **vertical market portals**. **General-purpose portals attempt to attract a very large general audience and then retain the audience on-site by providing in-depth vertical content channels, such as information on news, finance, autos, movies, and weather.** General-purpose portals typically offer **search engines, free e-mail, personal home pages, chat rooms, community-building software, and bulletin boards.** Vertical content channels on general-purpose portal sites offer content such as sports scores, stock tickers, health tips, instant messaging, automobile information, and auctions.

general-purpose portals

attempt to attract a very large general audience and then retain the audience on-site by providing in-depth vertical content

INSIGHT ON BUSINESS

VERIZON DOUBLES DOWN ON PORTALS

In the early years of the Internet, portals were among the most high-profile of business models. AOL and Yahoo were two of the most prominent.

In 2000, Time Warner bought AOL for \$168 billion and Yahoo was worth about \$128 billion. However, as the years passed, Google developed a stranglehold on the search market and social networks such as Facebook have largely usurped the role that portals originally played in online life. Both AOL and Yahoo struggled and undertook various efforts to transform their businesses to make them more relevant in today's online environment.

Over the last few years, Verizon, the U.S. broadband and wireless telecommunications giant, has been facing a similar issue, but for different reasons. Verizon is a direct descendant of the original Bell Telephone Company of the early 20th century. Today, Verizon is the largest wireless cell phone service provider in the United States, with 140 million subscribers (46% of the market), followed by AT&T with 128 million (33%). Other major providers include T-Mobile and Sprint. Verizon also controls around 35% of the landline (wireline) market. In 2015, Verizon generated revenue of \$131 billion. Most of this (70%) came from its wireless cell phone network segment. The rest comes from its wireline segment, which owns and operates the copper and fiber optic cables in buildings, underground, and under the sea that are used by major corporations and Internet providers.

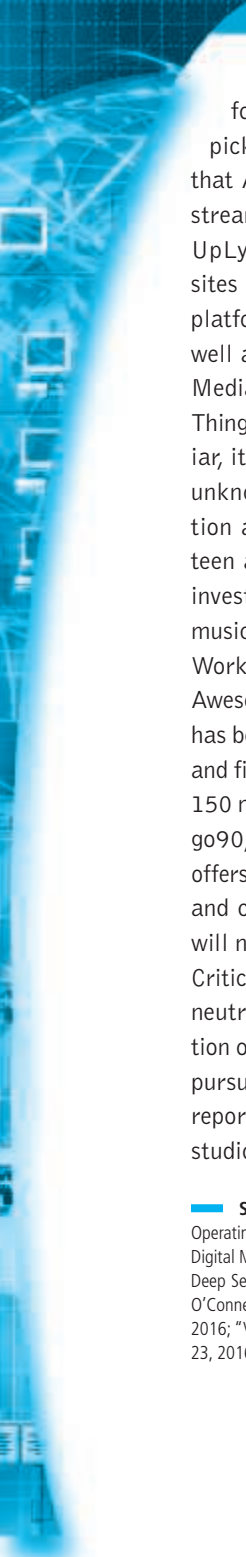
Despite Verizon's obvious size and market dominance, it is facing troubled times in the wireless business. Competitors like AT&T, Sprint, and T-Mobile have put a lid on the fees Verizon can charge wireless customers. Revenue in the wireless segment grew only 4% in 2015, while the wireline

segment lost 1.5%. Microsoft, Google, Apple, Skype, and Facebook offer alternative communications over the Internet that drain revenue from all of the wireless telephone networks. The growth of Wi-Fi connections in urban areas also competes with Verizon cellular wireless networks. Smartphones typically default to Wi-Fi when available. The market for wireless experienced extraordinary growth following the introduction of the Apple iPhone in 2007, but the market for connecting people with mobile cell voice, text, and video is approaching saturation, and is no longer a growth story. It has become clear that there's more money in owning the media content, the audience, and the brand than owning the pipes. So in a remarkable, unprecedented corporate makeover, Verizon has decided to become an online media and digital advertising company, a business in which it has no prior experience!

To achieve its plan of becoming a major player in online media and advertising, Verizon needs to build an audience. To attract the audience, it needs digital content, preferably video, which seems to have an insatiable online audience. The plan target is 2 billion viewers by 2020. With billions of eyeballs, Verizon hopes to become a media and advertising power house that can challenge Facebook and YouTube (Google) for a sizable chunk of the burgeoning online ad market, which is growing at over 20% annually. Now that's high-tech growth country! Analysts wondered how a phone company could become an Internet media and ad company. The answer: buy them.

To put this plan in to action, in 2014, Verizon bought AOL for \$4.4 billion. Analysts at the time wondered why Verizon would buy a fading star portal. The answer would soon become clear: an online audience of 400 million and lots of digital content. In addition, AOL also operated one of the

(continued)



largest digital advertising firms (AOL Platforms). With the AOL purchase, Verizon also picked up dozens of Internet content companies that AOL had previously acquired, such as video streaming firms EdgeCast Networks, OnCue, and UpLynk; blogs Engadget and TechCrunch; news sites like Huffington Post, along with three video platforms (5MinMedia, AdapTV, and Vidible); as well as a mobile advertising company Millennial Media, and a social sharing technology company, Thing Labs. If some of these names are unfamiliar, it's because they are mostly small, relatively unknown, short-form, low-budget video production and distribution companies focused on the teen and young adult audience. Verizon has also invested along with Hearst in ComplexMedia, a music and pop-culture site and along with DreamWorks Animation and Hearst in AwesomenessTV. AwesomenessTV started as a YouTube channel and has begun to create original web series, TV shows, and films aimed at teenagers. AwesomenessTV has 150 million subscribers. In 2015, Verizon launched go90, a free, ad-supported streaming service that offers original series such as *The Runner*, *Tween Fest*, and comedy shows. Verizon customers' accounts will not be charged minutes for using the service. Critics claim this is in violation of the FCC's new net neutrality regulations, which prohibit discrimination on basis of platform or content. Verizon is also pursuing more mainstream content and has been reported to be meeting with Hollywood production studios seeking original long-form programming

that is suited to digital distribution. Hulu, Amazon, Netflix, and Google are the targets.

In 2016, expanding on this strategy, Verizon agreed to purchase Yahoo, another failing portal, for \$4.83 billion. Yahoo was unsuccessful in developing its own original content, but is the king of display ads and supporting technology, with over 1 billion users worldwide, including 600 million who access the site via a mobile device. The acquisition is scheduled to close sometime during the first quarter of 2017.

If Verizon is successful in attracting 2 billion viewers by 2020, it can enter the rapidly growing business of Internet advertising, and compete with Facebook, Google, Microsoft, and other content companies in the streaming video market. Verizon's geolocation technology, which is built into its mobile network and keeps track of every mobile user around the clock, can be used to target users based on their activities and location. As the leading wireless provider, Verizon knows more about the location of people and things, and how they got there, than the people or things themselves.

There are plenty of doubters that Verizon can effectively manage all these acquisitions and become a multifaceted portal conglomerate. Verizon's supposed unique advantage is that it has a mobile customer base of 144 million customers and knows their location. So do Google Maps and Apple's iPhones. It is unclear at this point if Verizon can compete against the reigning Internet titans who now dominate social networks, web media, and online advertising. But it will be exciting to find out how this bet turns out.

SOURCES: "Yahoo and the Online Universe According to Verizon," by David Gelles, *New York Times*, July 30, 2016; "Verizon to Acquire Yahoo's Operating Business," PRNewswire, July 25, 2016; "The Problem with Verizon-Yahoo," by Erin Griffith, *Fortune*, July 25, 2016; "Inside Verizon's Gamble on Digital Media," by Ryan Knutson and Deepa Seetharaman, *Wall Street Journal*, July 24, 2016; "Verizon Finalizes \$4.8 Billion Yahoo Deal," Ryan Knutson and Deep Seetharaman, *Wall Street Journal*, July 24, 2016; "Verizon's Multi-Billion Dollar Play to Take On Netflix, Amazon, Google, and Facebook," by Ainsley O'Connell, *Fast Company*, May 26, 2016; "Verizon Settles With F.C.C. Over Hidden Tracking via 'Supercookies,'" by Cecilia Kang, *New York Times*, March 7, 2016; "Verizon Communications Inc. Form 10-K filed with the Securities and Exchange Commission for the Fiscal Year Ended December 31, 2015," February 23, 2016; "All the Media Companies That Belong to Verizon Now," by Kate Knibbs, *Gizmodo*, May 12, 2015.

Vertical market portals (sometimes also referred to as destination sites or vortals) attempt to attract highly focused, loyal audiences with a deep interest in either community or specialized content—from sports to the weather. In addition to their focused content, vertical market portals have recently begun adding many of the features found in general-purpose portals. For instance, in addition to being a social network, you can also think of Facebook as a portal—the home page for millions of users, and a gateway to the Internet. Facebook is an affinity group portal because it is based on friendships among people. Facebook offers e-mail, search, games, and apps.

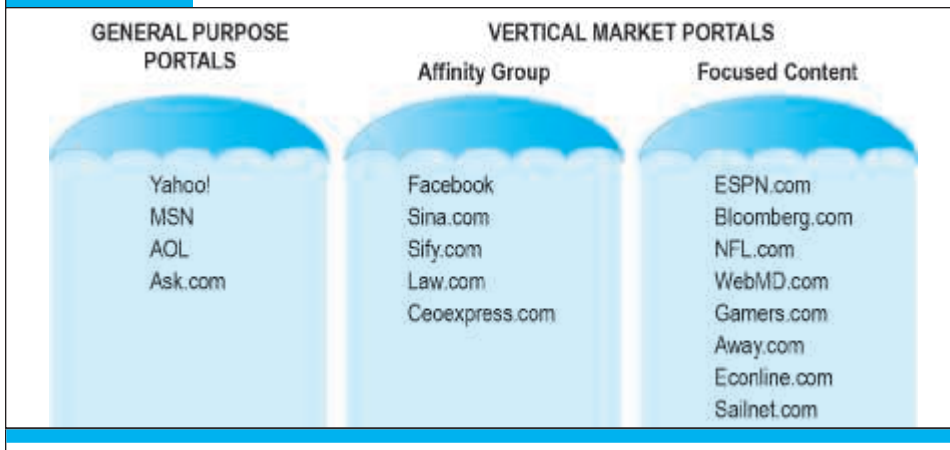
The concentration of audience share in the portal market reflects (in addition to network effects) the limited time budget of consumers. This limited time budget works to the advantage of general-purpose portals. Consumers have a finite amount of time to spend on the Web, and as a result, most consumers visit fewer than 30 unique domains each month. Facing limited time, consumers concentrate their visits at sites that can satisfy a broad range of interests, from weather and travel information, to stocks, sports, retail shopping, and entertainment content.

General-purpose sites such as Yahoo try to be all things to all people and attract a broad audience with both generalized navigation services and in-depth content and community efforts. For instance, Yahoo has become the Web's largest source of news: more people visit Yahoo News than any other news site including online newspapers. Yet recent changes in consumer behavior on the Web show that consumers are spending less time “surfing the Web” and on general browsing, and more time doing focused searches, research, and participating in social networks. These trends will advantage special-purpose, vertical market sites that can provide focused, in-depth community and content.

As a general matter, the general-purpose portals are very well-known brands, while the vertical content and affinity group portals tend to have less well-known brands. **Figure 11.5** lists examples of general-purpose portals and the two main types of vertical market portals.

vertical market portals
attempt to attract highly focused, loyal audiences with a deep interest in either community or specialized content

FIGURE 11.5 TWO GENERAL TYPES OF PORTALS: GENERAL-PURPOSE AND VERTICAL MARKET PORTALS



There are two general types of portals: general-purpose and vertical market. Vertical market portals may be based on affinity groups or on focused content.

TABLE 11.7 TYPICAL PORTAL REVENUE SOURCES	
PORTAL REVENUE SOURCE	DESCRIPTION
General advertising	Charging for impressions delivered
Tenancy deals	Fixed charge for guaranteed number of impressions, exclusive partnerships, “sole providers”
Commissions on sales	Revenue based on sales at the site by independent providers
Subscription fees	Charging for premium content
Applications and games	Games and apps are sold to users; advertising is placed within apps

PORTAL BUSINESS MODELS

Portals receive income from a number of different sources. The revenue base of portals is changing and dynamic, with some of the largest sources of revenue declining. **Table 11.7** summarizes the major portal revenue sources.

The business strategies of both general-purpose and vertical portals have changed greatly because of the rapid growth in search engine advertising and intelligent ad placement networks such as Google’s AdSense, which can place ads on thousands of websites based on content. General portal sites such as AOL and Yahoo did not have well-developed search engines, and hence have not grown as fast as Google, which has a powerful search engine. Microsoft, for instance, has invested billions of dollars in its Bing search engine to catch up with Google. On the other hand, general portals have content, which Google did not originally have, although it added to its content by purchasing YouTube and adding Google sites devoted to news, financial information, images, and maps. Facebook users stay on-site and linger three times as long as visitors to traditional portals like Yahoo. For this reason social network sites, Facebook in particular, are direct competitors of Yahoo, Google, and the other portals. Yahoo has struggled in the last three years to grow revenues and earnings despite the fact that its unique visitor count has held steady with Google’s. One part of the problem is the falling price of display ads, which are the mainstay of Yahoo’s ad platform. Yahoo shows more display ads on its sites than any other web destination. Another key issue is declining user engagement with materials on the site and the amount of time spent on the site. To address these issues, Yahoo has made a number of acquisitions including Aviate, Tumblr, and Flickr, and launched digital magazines like Yahoo Food and Yahoo Tech that curate content from around the Web. The key to display ad revenue is content and engagement: the more you can show users, the longer they stay on your site, the more ad revenue can be generated. So far, Yahoo and the other general portal sites have not been able to compete with social network sites on these dimensions of engagement and time on site. After several years of pursuing unsuccessful new strategies, Yahoo agreed to sell itself to Verizon in 2016.

The survival strategy for general-purpose portals in the future is therefore to develop deep, rich vertical content in order to reach and engage customers at the site. This involves hiring professional journalists rather than relying on bloggers who write listicle articles, and offering more quality entertainment in the form of movies, TV series, and music. The strategy for much smaller vertical market portals is to put together a collection of vertical portals to form a vertical portal network, a collection of deep, rich content sites. The strategy for search engine sites such as Google is to obtain more content to attract users for a long time and expose them to more ad pages (or screens).

11.4

CASE STUDY

eBay Evolves

When you hear someone mention online auctions, the first site that comes to mind is likely eBay. Founded in 1995 as an offbeat, quirky place to buy and sell almost anything via auctions, eBay now derives the majority of its revenue from traditional e-commerce.

As the company continues to model its business after competitors such as Amazon and Alibaba, eBay has banned the sales of quirkier services like tarot card readings and magic spells, and has instituted a rewards program with prominent retail chains like Dick's Sporting Goods and Toys "R" Us.

The transformation began in November 2007, when former CEO Meg Whitman exited and was replaced by John Donahoe. The company had already begun to stall, and the trend continued through 2009. For many buyers, the novelty of online auctions had worn off, and they were returning to easier and simpler methods of buying fixed-price goods from retailers such as Amazon, which, by comparison, had steady growth during the same time period. Search engines and comparison shopping sites were also taking away some of eBay's auction business by making items easier to find on the Web.

Donahoe quickly found that dramatically altering the business model of an Internet company is never easy, particularly when that company is one of the most recognizable sites on the Web. His three-year revival plan moved eBay away from its origins as an



online flea market, and at first it began to resemble an outlet mall where retailers sold out-of-season, overstocked, refurbished, or discontinued merchandise. From there it was a straightforward progression to partnering with retail chains to simply serve as another channel for current merchandise.

Small sellers were encouraged to shift away from the auction format and move toward the fixed-price sales model. The fee structure was adjusted, listing fees for fixed-price sales were lowered, improvements were made to the search engine, and rather than displaying ending auctions first, a formula was devised that took into account price and seller reputation so that highly rated merchants appeared first and received more exposure.

Unsurprisingly, the growing pains during this period included increasing complaints from sellers about excessive fees and eBay's favoritism toward big retailers. The hundreds of thousands of people who supported themselves by selling on eBay and many millions more who used eBay to supplement their income often felt slighted. With its stock continuing to drop, analysts' faith that Donahoe could turn things around dwindled. This pessimism failed to account for eBay's history of sensible growth marked by a number of canny purchases.

Its signature purchase was, of course, PayPal, whose payment services enable the exchange of money between individuals over the Internet. This acquisition was the key to eBay's endurance through the lean years, protecting it from weakness in its auction business, and the propeller that pushed it towards the future. PayPal has accounted for over 40% of eBay's revenues at its peak, and was a significant factor in eBay's growth.

eBay recognized the coming mobile revolution even before the first iPhone or the establishment of the App Store, according to Olivier Ropars, senior director of Mobile Commerce. This prescience resulted in eBay achieving its 100 millionth app download and 100 millionth mobile listing relatively early on, in 2012. Dating back to 2010, eBay has been actively acquiring companies specializing in mobile technologies, such as barcode scanning app RedLaser, mobile app developer Critical Path, mobile payment and billing firm Zong, and mobile payment startup Fig Card. In 2013, eBay acquired mobile payment gateway Braintree for \$800 million. Braintree's technology allows eBay consumers to more easily make payments on smartphones and tablets, and the acquisition also eliminated a major competitor in that space for PayPal. In 2015, eBay introduced an app for the Apple Watch that allows users to see an overview of their notifications and bid statuses. The company also rolled out more updates for their iOS and Android apps that improve the quality of search results. In 2016, eBay remains on the cutting edge of online retail, redesigning its core mobile platform and adding biometric touch identification support, launching its Marketplace app for Android Wear wearable devices, and releasing a virtual reality feature on StubHub that allows customers to see their prospective seats from any angle. Over 50% of eBay's business now involves a mobile device, and the company continues to make improvements to the mobile experience across all of its different services.

While many other acquisitions through the years have also helped to transform eBay from an online garage sale to a mainstream competitor with Amazon, its adoption of the "social, mobile, local" driving theme has been central to its survival. Positioning itself at the center of the online—offline—mobile triangle by offering a wide variety of

SOURCES: "PayPal Introduces an SDK for PayPal Here, Its Square-like Credit Card Reader," by Roberto Baldwin, thenextweb.com,

September 4, 2014; "eBay's 900 Million Dollar Question," by Chad Henage, Motley Fool, June 17, 2014; "Alibaba Takes on eBay, Etsy with U.S.-based Shopping Site," by Gail Sullivan, *Washington Post*, June 11, 2014; "Web? Store? Mobile? Shoppers Want It All," by Don Davis, *Internetretailer.com*, June 11, 2014; "Did Panda Really Beat Up On eBay?" by Thad Rueter, *Internetretailer.com*, June 9, 2014; "eBay Plays the Field," by Katie Evans, *Internetretailer.com*, June 2, 2014; "How the Once Impregnable eBay Fell Victim to Hackers (and You Can Too)," by Jeremy Quittner, *Inc.com*, May 30, 2014; "eBay Reports 13% Sales Growth and Rejects PayPal Spinoff," by Katie Evans, *Internetretailer.com*, January 22, 2014; "Behind eBay's \$800M Buy: Braintree will Replace PayPal's Developer Platform," by Kevin Fitchard, *Gigaom.com*, September 26, 2013; "Amazon, eBay Lead Way as E-Commerce Sales Still Surge," by Brian Deagon, *Investor's Business Daily*, July 2, 2013; "eBay Hits 100m Mobile App Download Mark," by Dervedia Thomas, *Dailydealmedia.com*, September 29, 2012; "eBay: We Need to Behave More Like a Retailer," by Sarah Shearman, *Tamebay.com*, September 25, 2012; "eBay Logo Gets a Refresh; The Time Felt Right After 17 Years," by Mark Tyson, *Hexus.com*, September 14, 2012; "eBay Bans Magic Spells and Potions," by Katy Waldman, *Slate.com*, August 17, 2012; "Behind eBay's Comeback," by James B. Stewart, *New York Times*, July 27, 2012; "Bill Me Later, eBay's Credit Version of PayPal, Helps Company's Profits but Exposes It to Risk," by Alistair Barr, *MercuryNews.com*, July 12, 2012; "PayPal Strength Helps eBay Exceed Forecasts," by Somini Sengupta, *New York Times*, April 18, 2012; "eBay Favors Big-Box Retailers in Holiday Promotions," by Ina Steiner, *eCommerce-Bytes.com*, December 16, 2011; "How Jack Abraham Is Reinventing eBay," by Danielle Sacks, *Fast Company*, June 22, 2011; "Connecting the Dots on eBay's Local Shopping Strategy," by Leena Rao, *Techcrunch.com*, May 15, 2011; "eBay CEO Sees Opportunities in Online and Offline Commerce," by Scott Morrison, *Wall Street Journal*, February 10, 2011.

services that enable merchants to more easily integrate their cross-channel retailing has been the key to eBay's resurgence and to its continued success.

In 2016, the company has also started the process of modernizing its platform with analytical tools. First, the company has started to convert its catalog of items from its traditional unstructured "listing" format, where two identical items can appear totally different to shoppers, to a structured data format. This will allow eBay to more easily gain information about different items and about purchasing trends. eBay is also using machine learning to customize, update, and generally improve its product pages, as well as to fine-tune its search capability beyond simply matching search terms with keywords and tags. To support these efforts, in 2016, the company purchased machine-learning startup SalesPredict, whose technology helps businesses predict consumer buying behavior and sales conversion. Finally, the company's revamped Seller Hub will offer many of these analytical tools and metrics to individual sellers, including inventory, order, and listing management, performance insights, and streamlined business process management.

However, eBay's return to prominence is not without continuing challenges. In 2014, eBay was the victim of a hacking attack that compromised the information of nearly 150 million of its customers. PayPal was unaffected, and the company doesn't believe that any financial information was stolen, but the incident underscored the need for eBay to remain vigilant with its security measures. eBay sales decreased steeply in the wake of the breach, dropping 5.4% in 10 days. Competitors are also ramping up their efforts to battle eBay, with Amazon continuing to focus on third-party sales and Alibaba announcing a U.S.-based site to compete with eBay called 11 Main. What's more, Google rolled out an update to its search algorithm, reducing eBay's search traffic by as much as 33%. eBay hopes that standardizing its product pages will also help improve its rankings in Google searches.

In 2015, eBay elected to spin off PayPal as its own separate company, leaving eBay with its Marketplaces segment, its StubHub ticket sales segment, and a handful of other business units. Although Donahoe and the rest of eBay's leadership had resisted a spinoff for years, the move was prompted by a desire for PayPal to distinguish itself from eBay and become more agile within the rapidly-developing marketplace of online payments. Donahoe also stepped down as CEO of eBay to mark the transition, with the former head of its Global Marketplaces unit, Devin Wenig, taking his place. As part of the split, eBay has agreed to route 80% of its sales through PayPal, but PayPal is free to pursue deals with other merchants, potentially boosting its market share even further.

Many investors believed that PayPal had been the true driver of eBay's bottom line. But while analysts had prepared themselves for disappointing earnings, the company has instead posted several straight quarters of sales growth under Wenig as of 2016. This includes a 5.7% increase over its earnings from the previous year in the second quarter of 2016, with \$2.23 billion in revenue, up from \$2.11 billion in 2015. The company also reported that it expected continued growth for the upcoming quarters. Despite Amazon's ongoing dominance in online retail, eBay remains one of the most trusted online brands and e-commerce leaders, and it has worked hard to improve its marketplace design and offerings for dedicated users, including eBay Now, its new same-day delivery program. Will eBay be able to respond to these new challenges as well as it has to those in the past without PayPal to bolster it? After some ups and downs, eBay appears to be on a winning trajectory once again.

Case Study Questions

1. Contrast eBay's original business model with its current business model.
2. What are the problems that eBay is currently facing? How is eBay trying to solve these problems?
3. Are the solutions eBay is seeking to implement good solutions? Why or why not? Are there any other solutions that eBay should consider?
4. Who are eBay's top competitors online, and how will eBay's strategy help it compete?

11.5 REVIEW

KEY CONCEPTS

- Describe the different types of social networks and online communities and their business models.
 - Social networks involve a group of people, shared social interaction, common ties among members, and a shared area for some period of time. An online social network is one where people who share common ties can interact with one another online.
 - The different types of social networks and communities and their business models include:
 - *General communities*: Members can interact with a general audience segmented into numerous different groups. Most general communities began as non-commercial subscription-based endeavors, but many have been purchased by larger community portal sites.
 - *Practice networks*: Members can participate in discussion groups and get help or information relating to an area of shared practice, such as art, education, or medicine. These generally have a nonprofit business model in which they simply attempt to collect enough in subscription fees, sales commissions, and limited advertising to cover the cost of operations.
 - *Interest-based communities*: Members can participate in focused discussion groups on a shared interest. The advertising business model has worked because the targeted audience is attractive to marketers. Tenancy and sponsorship deals provide another similar revenue stream.
 - *Affinity communities*: Members can participate in focused discussions with others who share the same affinity or group identification. The business model is a mixture of subscription revenue from premium content and services, advertising, tenancy/sponsorships, and distribution agreements.
 - *Sponsored communities*: Members can participate in online communities created by government, nonprofit, or for-profit organizations for the purpose of pursuing organizational goals. They use community technologies and techniques to distribute information or extend brand influence. The goal of a branded product site is to increase offline product sales. These sites do not seek to make a profit and are often cost centers.
- Describe the major types of auctions, their benefits and costs, how they operate, when to use them, and the potential for auction abuse and fraud.
 - Auctions are markets where prices vary (dynamic pricing) depending on the competition among the participants who are buying or selling products or services. They can be classified broadly as C2C or B2C,

although generally the term *C2C auction* refers to the venue in which the sale takes place, for example, a consumer-oriented website such as eBay, which also auctions items from established merchants. A *B2C auction* refers to an established online merchant that offers its own auctions. There are also numerous B2B online auctions for buyers of industrial parts, raw materials, commodities, and services. Within these three broad categories of auctions are several major auction types classified based upon how the bidding mechanisms work in each system:

- *English auctions*: A single item is up for sale from a single seller. Multiple buyers bid against one another within a specific time frame with the highest bidder winning the object as long as the high bid has exceeded the reserve bid set by the seller, below which he or she refuses to sell.
- *Dutch Internet auctions*: Sellers with many identical items for sale list a minimum price or starting bid, and buyers indicate both a bid price and a quantity desired. The lowest winning bid that clears the available quantity is paid by all winning bidders. Those with the highest bid are assured of receiving the quantity they desire but only pay the amount of the lowest successful bid (uniform pricing rule).
- *Name Your Own Price or reverse auctions*: Buyers specify the price they are willing to pay for an item, and multiple sellers bid for their business. This is one example of discriminatory pricing in which winners may pay different amounts for the same product or service depending on how much they have bid.
- *Penny (bidding fee) auctions*: Bidders pay a non-refundable fee to purchase bids.
- Benefits of auctions include: liquidity, price discovery, price transparency, market efficiency, lower transaction costs, consumer aggregation, network effects, and market-maker benefits.
- Costs of auctions include: delayed consumption, monitoring costs, equipment costs, trust risks, and fulfillment costs.
- Auction sites have sought to reduce these risks through various methods including rating systems, watch lists, and proxy bidding.
- Auctions can be an appropriate channel for businesses to sell items in a variety of situations. The factors for businesses to consider include the type of product, the product life cycle, channel management, the type of auction, initial pricing, bid increments, auction length, number of items, price allocation, and closed versus open bidding.
- Auctions are particularly prone to fraud, which produces information asymmetries between buyers and sellers. Some of the possible abuses and frauds include bid rigging, price matching, defensive shill feedback, offensive shill feedback, feedback extortion, transaction interference, bid manipulation, non-payment after winning, shill bidding, transaction non-performance, non-selling sellers, and bid siphoning.

■ Describe the major types of Internet portals and their business models.

- Portals are gateways to billions of web pages available on the Internet. Originally, their primary purpose was to help users find information on the Web, but they evolved into destination sites that provided a myriad of content from news to entertainment. Today, portals serve three main purposes: navigation of the Web (search), content, and commerce.
- Among the major portal types are:
 - *Enterprise portals*: Corporations, universities, churches, and other organizations create these sites to help employees or members navigate to important content such as corporate news or organizational announcements.
 - *General-purpose portals*: Examples are AOL, Yahoo, and MSN, which try to attract a very large general audience by providing many in-depth vertical content channels. Some also offer ISP services on a subscription basis, search engines, e-mail, chat, bulletin boards, and personal home pages.
 - *Vertical market portals*: Also called destination sites, they attempt to attract a highly focused, loyal audience with an intense interest in either a community they belong to or an interest they hold.

Vertical market portals can be divided into two main classifications, although hybrids that overlap the two classifications also exist.

- *Affinity groups*: Designed to serve aggregates of people who identify themselves by their attitudes, values, beliefs, and behavior.
- *Focused content portals*: These sites contain in-depth information on a particular topic that all members are interested in. They can provide content on such broad topics as sports, news, weather, entertainment, finance, or business, or they can appeal to a much more focused interest group such as boat, horse, or video game enthusiasts.
- Portals receive revenue from a number of different sources. The business model is presently changing and adapting to declines in certain revenue streams, particularly advertising revenues. Revenue sources can include general advertising, tenancy deals, subscription fees, and commissions on sales.
- The survival strategy for general-purpose portals is to develop deep, rich vertical content in order to attract advertisers to various niche groups that they can target with focused ads. The strategy for the small vertical market portals is to build a collection of vertical portals, thereby creating a network of deep, rich content sites for the same reason.

QUESTIONS

1. What do social networks, auctions, and portals have in common?
2. What are the four defining elements of a social network—online or offline?
3. Why is Pinterest considered a social network, and how does it differ from Facebook?
4. What are three mobile social networks?
5. Why are mobile social networks growing so fast?
6. What are two measures that can be used to understand the importance of social networks and to compare them to other Internet experiences?
7. What is an affinity community, and what is its business model?
8. List and describe four different types of auctions.
9. What is the difference between a C2C and a B2C auction?
10. How does a Name Your Own Price auction, such as Priceline's, work?
11. List and briefly explain three of the benefits of auction markets.
12. What are the four major costs to consumers of participating in an auction?
13. Why has the FTC warned consumers about penny (bidding fee) auctions?
14. What is herd behavior and how does it impact auctions?
15. Name and describe five types of possible abuses and frauds that may occur with auctions.
16. What types of products are well suited for an auction market? At what points in the product life cycle can auction markets prove beneficial for marketers?
17. What three characteristics define a portal site today?
18. What are the two main types of vertical market portals, and how are they distinguished from one another?
19. List and briefly explain the main revenue sources for the portal business model.
20. Why has Yahoo struggled in the last three years?

PROJECTS

1. Find two examples of an affinity portal and two examples of a focused-content portal. Prepare a presentation explaining why each of your examples should be categorized as an affinity portal or a focused-content portal. For each example, surf the site and describe the services each site provides. Try to determine what revenue model each of your examples is using and, if possible, how many members or registered visitors the site has attracted.

2. Examine the use of auctions by businesses. Go to any auction site of your choosing and look for outlet auctions or auctions directly from merchants. Research at least three products for sale. What stage in the product life cycle do these products fall into? Are there quantity purchasing requirements? What was the opening bid price? What are the bid increments? What is the auction duration? Analyze why these firms have used the auction channel to sell these goods and prepare a short report on your findings.
3. Visit one for-profit and one nonprofit sponsored social network. Create a presentation to describe and demonstrate the offering at each site. What organizational objectives is each pursuing? How is the for-profit company using community-building technologies as a customer relations management tool?
4. Visit one of the social networks listed in Table 11.1 and compare it to Facebook. In what ways is it similar to Facebook, and in what ways is it different? Which do you prefer, and why?

REFERENCES

- Arkes, H. R., and L. Hutzler. "The Role of Probability of Success Estimates in the Sunk Cost Effect." *Journal of Behavioral Decisionmaking* (2000).
- Bailey, Brian P., Laura J. Gurak, and Joseph Konstan. "Do You Trust Me? An Examination of Trust in Computer-Mediated Exchange," In *Human Factors and Web Development*, 2nd Edition. Mahwah, NJ: Lawrence Erlbaum (2002).
- Barnes, Nora, Ava Lescault, and Glenn Holmes. "The 2015 Fortune 500 and Social Media: Instagram Gains, Blogs Lose." University of Massachusetts (Dartmouth) (2015).
- Bloomapp.co "About Us." (accessed October 10, 2016).
- Compete.com. "August 2016 Unique Visitors." (accessed October 8, 2016a).
- comScore. "Top 50 Multi-Platform Properties (Desktop and Mobile) August 2016." (August 2016a).
- comScore. "The 2016 U.S. Mobile App Report." (2016b).
- Consumerreports.org. "With Penny Auctions, You Can Spend a Bundle But Still Leave Empty-Handed." (June 30, 2014).
- Cormen, Thomas H. and Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, 3rd Edition* (MIT Press) 3rd Edition. MIT Press, 2009.
- Data Center Knowledge. "The Facebook Data Center FAQ." Datacenterknowledge.com (September 16, 2016).
- Dholakia, Utpal, and Kerry Soltysinski. "Coveted or Overlooked? The Psychology of Bidding for Comparable Listings in Digital Auctions." *Marketing Letters* (2001).
- eBay, Inc. "Form 10-K for the Fiscal Year Ended December 31, 2015." Filed with the Securities and Exchange Commission. (February 1, 2016).
- eMarketer, Inc. "US Social Network Users and Penetration," 2015–2020." (August 3, 2016a).
- eMarketer, Inc. "US Mobile Phone Facebook Users and Penetration, 2015–2020." (August 5, 2016b).
- eMarketer, Inc. (Cindy Liu). "Worldwide Social Network Users: eMarketer's Estimates for 2016." (June 2016c).
- eMarketer, Inc. "US Facebook Users, by Age, 2015–2020." (August 3, 2016d).
- eMarketer, Inc. "US Digital Ad Spending, by Format, 2015–2020." (August 24, 2016e).
- eMarketer, Inc. "US Social Network Ad Revenues, by Venue, 2015–2018 (millions, % change and % of total)." (September 1, 2016f).
- Facebook. "Newsroom/Company Info." (accessed October 5, 2016).
- Hafner, Katie. "The Epic Saga of The Well: The World's Most Influential Online Community (and It's Not AOL)." *Wired* (May 1997).
- Hagel, John III, and Arthur G. Armstrong. *Net Gain: Expanding Markets Through Virtual Communities*. Cambridge, MA: Harvard Business School Press (1997).
- Hanson, Ward, and D. S. Putler. "Hits and Misses: Herd Behavior and Online Product Popularity." *Marketing Letters* (1996).
- Hillery, George A. "Definitions of Community: Areas of Agreement." *Rural Sociology* (1955).
- Hiltzik, Michael. *Dealers of Lightning: Xerox PARC and the Dawn of the Computer Age*. New York: Harper Collins (1999).
- Instagram. "Press News." (accessed October 5, 2016).
- Kiesler, Sara. "The Hidden Messages in Computer Networks." *Harvard Business Review* (January–February 1986).
- Kiesler, Sara, Jane Siegel, and Timothy W. McGuire. "Social Psychological Aspects of Computer-Mediated Communication." *American Psychologist* (October 1984).
- Kollock, Peter. "The Production of Trust in Online Markets." In *Advances in Group Processes* (Vol 16), edited by E. J. Lawler, M. Macy, S. Thyne, and H. A. Walker. Greenwich, CT: JAI Press (1999).

- Krishnamurthy, Sandeep. "An Empirical Study of the Causal Antecedents of Customer Confidence in E-tailers." *First Monday* (January 2001).
- Laudon, Kenneth C., and Jane P. Laudon. *Management Information Systems: Managing the Digital Firm. 15th edition*. Upper Saddle River, NJ, Prentice Hall (2016).
- Liu, Yi, and Juliana Sutanto. "Buyers' Purchasing Time and Herd Behavior on Deal-of-the-Day Group-buying Websites." *Electronic Markets* (June 2012).
- Nikander, Pekka, and Kristina Karvonen. "Users and Trust in Cyberspace." In the Proceedings of Cambridge Security Protocols Workshop 2000, April 3–5, 2000, Cambridge University (2002).
- Parkes, David C., and Lyle Ungar. "Iterative Combinatorial Auctions: Theory and Practice." *Proceedings of the 17th National Conference on Artificial Intelligence (AAAI-00)* (2000).
- Rheingold, Howard. *Hosting Web Communities*. New York: John Wiley and Sons (1998). Also see Rheingold.com for more recent articles by Rheingold.
- Rheingold, Howard. *The Virtual Community*. Cambridge, MA: MIT Press (1993).
- Rosenbloom, Stephanie. "For the Plugged-In, Too Many Choices." *New York Times* (August 10, 2011).
- Simonson, Itamar, and Amos Tversky. "Choice in Context: Tradeoff Contrast and Extremeness Aversion." *Journal of Marketing Research*, Vol. 20, 281–287 (1992).
- Stanford Persuasive Technology Lab and Makovsky & Company. "Stanford-Makovsky Web Credibility Study 2002." Stanford Persuasive Technology Lab. (Spring 2002).
- United States Patent and Trademark Office. "U.S. Patent 7,827,208 B2." (November 2, 2010).