PEARSON

e-commerce

4/e

business. technology. society.

2008

kenneth c. laudon | carol guercio traver

MySpace and Facebook, and hundreds of other niche-oriented social networking sites, are emblematic of the new e-commerce. These sites and others, such as YouTube, Photobucket, and Second Life, are defining a new and vibrant model of e-commerce growing up alongside the more traditional e-commerce retail sales model exemplified by Amazon and eBay. In this new model, services—not retail goods—are provided both to subscribers as well as to business firms advertising to entirely new audiences. Second, the movement of eyeballs towards social networking and user-generated content sites means fewer viewers of television and Hollywood movies, and fewer readers of newspapers and magazines. Never before in the history of media have such large audiences been aggregated and made accessible. Social networks are a technology that is highly disruptive of traditional media firms. Social networks are becoming the place where new products can be introduced and where new sales can be achieved to highly targeted and segmented audiences with a precision heretofore impossible. Welcome to the new service-based e-commerce!

This is not the first time e-commerce has reinvented itself. In the past 10 years, e-commerce has gone through two transitions. The early years of e-commerce, during the late 1990s, were a period of business vision, inspiration, and experimentation, followed by the realization that establishing a successful business model based on those visions would not be easy, which then ushered in a period of retrenchment and reevaluation. The retrenchment led to the stock market crash of March 2000 to April 2001, when the stock market value of e-commerce, telecommunications, and other technology stocks plummeted in the space of a year by more than 90%. After the bubble burst, many people were quick to write off e-commerce and predicted that e-commerce growth would stagnate, and the Internet audience itself would plateau. But they were wrong. In this first transition, the surviving firms refined and honed their business models, ultimately leading to models that actually produced profits, resulting in e-commerce retail growth rates of over 25% per year.

The second transition is toward services such as creating and publishing photos, blogs and videos, and developing new communities and professional ties through network sites, even as the e-commerce retail goods trade continues to expand at 25% a year. And it probably safe to predict that this will not be the last transition for e-commerce.

1.1 E-COMMERCE: THE REVOLUTION IS JUST BEGINNING

In fact, the e-commerce revolution is just beginning. For instance, in 2007:

- Online consumer sales expanded by more than 25% to an estimated $225 billion (eMarketer, Inc., 2007a, b, c; Internet Retailer, 2007; Forrester Research, 2007a).
- The major source of online retail growth is now increased spending by existing online buyers rather than new buyers as trust and consumer confidence build. Shoppers are buying expensive, "high-touch" goods online such as consumer electronics, home furnishings, and apparel.

THE FIRST THIRTY SECONDS

It is important to realize that the rapid growth and change that has occurred in the first 12 years of e-commerce represents just the beginning—what could be called the first 30 seconds of the e-commerce revolution. The same technologies that drove the first decade of e-commerce (described in Chapter 3) continue to evolve at exponential rates. This underlying ferment in the technological groundwork of the Internet and Web presents entrepreneurs with new opportunities to both create new businesses and new business models in traditional industries, and also to destroy old businesses. Business change becomes disruptive, rapid, and even destructive, while offering entrepreneurs new opportunities and resources for investment.

Changes in underlying information technologies and continuing entrepreneurial innovation in business and marketing promise as much change in the next decade as seen in the last decade. The twenty-first century will be the age of a digitally enabled social and commercial life, the outlines of which we can barely perceive at this time. It appears likely that e-commerce will eventually impact nearly all commerce, and that most commerce will be e-commerce by the year 2050.

Is there a terminal velocity, or a terminal point, towards which e-commerce is hurtling? Can e-commerce continue to grow at its current rate indefinitely? It's possible that at some point, e-commerce growth may slow just because people have no more time to watch yet another Internet television show, or open more and more e-mail. However, currently, there is no foreseeable limit to the continued exponential development of the technology, or limits on the inventiveness of entrepreneurs to develop new uses for the technology. Therefore, for now at least, the disruptive process will continue.

Business fortunes are made—and lost—in periods of extraordinary change such as this. The next five years hold out extraordinary 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, offering the possibility of high rates of productivity and income growth in an inflation-free environment.

As a business or technology student, this book will help you perceive and understand the opportunities and risks that lie ahead. By the time you finish, you will be able to identify the technological, business, and social forces that have shaped the growth of e-commerce and extend that understanding into the years ahead.

WHAT IS E-COMMERCE?

e-commerce
the use of the Internet and the Web to transact business. More formally, digitally enabled commercial transactions between and among organizations and individuals

Our focus in this book is **e-commerce**—the use of the Internet and the Web to transact business. More formally, we focus on 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 and the Web. *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.

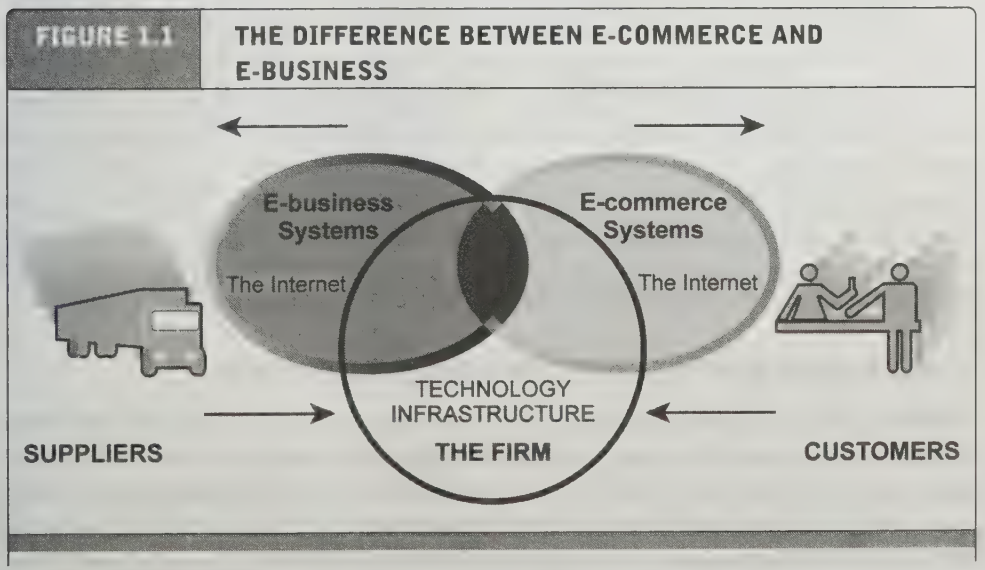
THE DIFFERENCE BETWEEN E-COMMERCE AND E-BUSINESS

There is a debate among consultants and academics 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's 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 that 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, for instance (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.

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

FIGURE 1.1 THE DIFFERENCE BETWEEN E-COMMERCE AND E-BUSINESS



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

WHY STUDY E-COMMERCE?

Why are there college courses and textbooks on e-commerce when there are no courses or textbooks on "TV Commerce," "Radio Commerce," "Direct Mail Commerce," "Railroad Commerce," or "Highway Commerce," even though these technologies had profound impacts on commerce in the twentieth century and account for far more commerce than e-commerce? Many colleges, including Massachusetts Institute of Technology (MIT), University of Michigan, Cornell University, University of California at Berkeley, and NSEAD Business School (France), are also developing courses on social interaction technologies and techniques, online social networks, online community development, and consumer-generated media. Is "YouTube 401" next?

The reason for the interest specifically in e-commerce is that e-commerce technology (discussed in detail in Chapters 3 and 4) is different and more powerful than any of the other technologies we have seen in the past century. E-commerce technologies—and the digital markets that result—promise to bring about some fundamental, unprecedented shifts in commerce. While these other technologies transformed economic life in the twentieth century, the evolving Internet and other information technologies will shape the twenty-first century.

Prior to the development of e-commerce, the marketing and sale of goods was a mass-marketing and sales force-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 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. One of the shifts that e-commerce appears to be bringing about is a large reduction in information asymmetry among all market participants (consumers and merchants). Preventing consumers from learning about costs, price discrimination strategies, and profits from sales becomes more difficult with e-commerce, and the entire marketplace potentially becomes highly price competitive.

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

EIGHT UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY

Table 1.2 lists eight unique features of e-commerce technology that both challenge traditional business thinking and 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. E-commerce technologies make it possible for merchants to know much more about

TABLE 1.2 EIGHT UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY

E-COMMERCE TECHNOLOGY DIMENSION	BUSINESS SIGNIFICANCE
Ubiquity—Internet/Web 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, namely Internet standards.	There is one set of technical media standards across the globe.
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 content generation and social networking.	New Internet social and business models enable user content creation .and distribution, and support social networks.

consumers and to be able to use this information more effectively than was ever true in the past. Potentially, online merchants can use this new 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 make it possible for merchants to know more about other

WEB 2.0: PLAY MY VERSION

Many of the unique features of e-commerce and the Internet come together in a set of applications and social technologies referred to as Web 2.0. The Internet started out as a simple network to support e-mail and file transfers among remote computers. Communication among experts was the purpose. The World Wide Web (the Web) started out as a way to use the Internet to display simple pages and allow the user to navigate among the pages by linking them together electronically. You can think of this as Web 1.0—the first Web. By 2007 something else was happening. The Internet and the Web have evolved to the point where users can now create, edit, and distribute content to millions of others; share with one another their preferences, bookmarks, and online personas; participate in virtual lives; and build online communities. This "new" Web is called by many "**Web 2.0**," and while it draws heavily on the "old" Web 1.0, it is nevertheless a clear evolution from the past.

Web 2.0
a set of applications and technologies that allows users to create, edit, and distribute content; share preferences, bookmarks, and online personas; participate in virtual lives; and build online communities

Let's look at some examples of Web 2.0 applications and sites:

- Photobucket zooms from 4 million to 50 million users and 3 billion consumer-generated photos to become the most popular Web photo posting site, offering users an easy way to post and send photos and video, and provides a convenient link to YouTube, MySpace, and blog pages (Photobucket.com, 2007).
- YouTube, owned by Google after a $1.65 billion purchase, grows to the largest online consumer-generated video posting site and still searches for a profitable business model. Over 65,000 videos are uploaded and 100 million videos are watched each day. This one site accounts for over 60% of all videos watched online (Reuters, 2006).
- MySpace ("A place for friends") rockets to the lead of online networking sites for 100 million Web socialites, and receives 49,000 consumer-generated videos each day to be shared with others, half of them from adults over 35 (News Corporation, 2007). Adult professional sites such as LinkedIn, Friendster, and Facebook attract additional millions of adults looking for online connections.
- Joost.com becomes the first Internet Television channel with financing of $50 million and agreements with networks to deliver TV programs to any Internet-connected device such as an iPod, MP3 player, cell phone, TV set top box, or any wirelessly connected PC or device. Suddenly TV is unleashed from cables, wires and national television networks or even local stations. Programming becomes user programming (Joost.com, 2007).
- Google attracts the largest Internet audience with 85 million daily U.S. users, and over 160 million international users, with a continual stream of innovations such as Google Maps, GoogleView (a photo database of U.S. neighborhoods from the street level), video and photo posting and sharing (more than 500 million photos), Gmail, and Google Scholar. Over 25% of Google search results on the world's top 20 brands provide links to consumer-generated content such as reviews, blogs, and photos (iProspect, 2007).

- Second Life is a 3-D virtual world built and owned by its residents who have established lives by building over 8.5 million avatars in "The World," spending Linden dollars, owning real estate, and building and sharing "creations," which include clothing, interior designs, or writing, among other items. Residents spend over $2 million real dollars each day to buy things on the site for their virtual lives, and convert the real dollars to Lindens (Secondlife.com, 2007).
- Wikipedia allows 35 million contributors in the United States alone to share their knowledge and in the process has become the most successful online encyclopedia, far surpassing early "professional" encyclopedias such as Encarta or even Britannica. Wikipedia is one of the largest collaboratively edited reference projects in the world. Garnering over 20% of the online reference market, Wikipedia relies on volunteers, makes no money, and accepts no advertising. The Wikimedia Foundation, Inc., a not-for-profit organization that relies on fund-raising and donations to survive, owns Wikipedia. Wikipedia is one of the top 10 most visited sites on the Web (Wikipedia.org, 2007).

What do all these applications and new sites have in common? First, they rely on user- and consumer-generated content. These are all "applications" created by people, especially people in the 18–34 year-old demographic, and heavily in the 7–17 age group as well. "Regular" people (not just experts or professionals) are creating, sharing, modifying, and broadcasting content to huge audiences. Second, easy search capability is a key to their success. Third, they are inherently highly interactive, creating new opportunities for people to socially connect to others. They are "social" sites because they support interactions among users. Fourth, they rely on broadband connectivity to the Web. Fifth, with the exception of Google, they are currently marginally profitable, and their business models unproven despite considerable investment. Sixth, they attract extremely large audiences when compared to traditional Web 1.0 applications, exceeding in many cases the audience size of national broadcast and cable television programs. These audience relationships are intensive and long-lasting interactions with millions of people. In short, they attract eyeballs in very large numbers. Hence, they present marketers with extraordinary opportunities for targeted marketing and advertising. They also present consumers with the opportunity to rate and review products, and entrepreneurs with ideas for future business ventures. Briefly, it's a whole new world from what has gone before. You'll learn more about Web 2.0 in later chapters.

TYPES OF E-COMMERCE

There are a variety of different types of e-commerce and many different ways to characterize these types. **Table 1.3** lists the five major types of e-commerce discussed in this book.[1]

[1]Business-to-Government (B2G) e-commerce can be considered yet another type of e-commerce. For the purposes of this text, we subsume B2G e-commerce within B2B e-commerce, viewing the government as simply a form of business when it acts as a procurer of goods and/or services.

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	Foodtrader is an independent third-party commodity exchange, auctions provider, and market information source that serves the food and agricultural industry.
C2C—Consumer-to-Consumer	On a large number of Web auction sites such as eBay, and listing sites such as Craigslist, consumers can auction or sell goods directly to other consumers.
P2P—Peer-to-Peer	BitTorrent is a software application that permits consumers to share videos and other high-bandwidth content with one another directly, without the intervention of a market maker as in C2C e-commerce.
M-commerce—Mobile commerce	Wireless mobile devices such as PDAs (personal digital assistants) and cell phones can be used to conduct commercial transactions.

For the most part, we distinguish different types of e-commerce by the nature of the market relationship—who is selling to whom. The exceptions are P2P and m-commerce, which are technology-based distinctions.

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. Even though B2C is comparatively small (about $225 billion in 2007), it has grown exponentially since 1995, and is the type of e-commerce that most consumers are likely to encounter. Within the B2C category, there are many different types of business models. Chapter 2 has a detailed discussion of seven different B2C business models: portals, online retailers, content providers, transaction brokers, service providers, and community providers.

Business-to-Business (B2B) E-commerce

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

Business-to-Business (B2B) e-commerce, in which businesses focus on selling to other businesses, is the largest form of e-commerce, with about $3.6 trillion in transactions in the United States in 2007. There was an estimated $16 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 could be huge. There are two primary business models used within the B2B arena:

This chapter examines the Internet and World Wide Web of today and tomorrow, how it evolved, how it works, and how the present and future infrastructure of the Internet and the Web enables new business opportunities.

The opening case about mashups and Web services illustrates how important it is for business people to understand how the Internet and related technologies work, and to be aware of what's new on the Internet. It could change your business drastically, and open up new opportunities as well. Operating a successful small business on the Web such as Simplest-Shop.com, or implementing key Web business strategies such as personalization, customization, market segmentation, and price discrimination, all require that business people understand Web technology and keep track of Web developments.

The Internet and its underlying computer technology is not a static phenomenon in history, but instead is changing very rapidly. The Internet happened, but it is also happening. Computers are merging with cell phone services; broadband access in the home and broadband wireless access to the Internet via wireless devices are expanding rapidly; self-publishing on the Web via blogging, social networking, and podcasting now engages millions of Internet users; and new software technologies such as Web services, grid computing, and peer-to-peer applications are being deployed. Looking forward a few years to the emerging Internet II of 2010, the business strategies of the future will require a firm understanding of these new technologies to deliver products and services to consumers.

3.1 THE INTERNET: TECHNOLOGY BACKGROUND

What is the Internet? Where did it come from, and how did it support the growth of the World Wide 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 those basics and then build from there. You'll also need to know about the business side of e-commerce, which you will learn about throughout this book.

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

As noted in Chapter 1, the **Internet** is an interconnected network of thousands of networks and millions of computers (sometimes called *host computers* or just *hosts*) linking businesses, educational institutions, government agencies, and individuals. The Internet provides approximately 1.2 billion people around the world (including about 175-200 million people in the United States) with services such as e-mail, newsgroups, shopping, research, instant messaging, music, videos, and news (Internetworldstats.com, 2007). 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 computer networks. The **World Wide Web**, or **Web** for short, is one of the Internet's most popular services, providing access to over 50 billion 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.

World Wide Web (Web)
one of the Internet's most popular services, providing access to over 50 billion Web pages

THE EVOLUTION OF THE INTERNET: 1961—THE PRESENT

Today's Internet has evolved over the last forty or so years. In this sense, the Internet is not "new;" it did not happen yesterday. Although journalists talk glibly about "Internet" time—suggesting a fast-paced, nearly instant, worldwide global change mechanism, in fact, it has taken over forty years of hard work to arrive at today's Internet.

The history of the Internet can be segmented into three phases (see **Figure 3.1**). In the first phase, the *Innovation Phase,* from 1961 to 1974, the fundamental building blocks of the Internet were conceptualized and then realized in actual hardware and software. The basic building blocks are: packet-switching hardware, client/server computing, and a communications protocol called TCP/IP (all described more fully later in this section). The original purpose of the Internet, when it was conceived in the 1960s, was to link large mainframe computers on different college campuses. This kind of one-to-one communication between campuses was previously only possible through the telephone system or postal mail.

In the second phase, the *Institutionalization Phase*, from 1975 to 1994, large institutions such as the Department of Defense and the National Science Foundation

FIGURE 3.1 STAGES IN THE DEVELOPMENT OF THE INTERNET

The Internet developed in three stages over a 40-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.

(NSF) provided funding and legitimization for the fledging invention called the Internet. Once the concepts behind the Internet had been proven in several government-supported demonstration projects, the Department of Defense contributed $1 million to further develop them into a robust military communications system that could withstand nuclear war. 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 ten-year-long $200 million expansion program.

In the third phase, the *Commercialization Phase*, from 1995 to the present, government agencies encouraged private corporations to take over and expand both the Internet backbone and local service to ordinary citizens—families and individuals across America and the world who were not students on campuses. By 2000, the Internet's use had expanded well beyond military installations and research universities. See **Table 3.1** for a closer look at the development of the Internet from 1961 on.

THE INTERNET: KEY TECHNOLOGY CONCEPTS

In 1995, the Federal Networking Council (FNC) took the step of passing a resolution formally defining the term *Internet* (see **Figure 3.2**).

Based on that definition, the Internet means 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.

RESOLUTION OF THE FEDERAL NETWORKING COUNCIL

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

'Internet' refers to the global information system that—

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

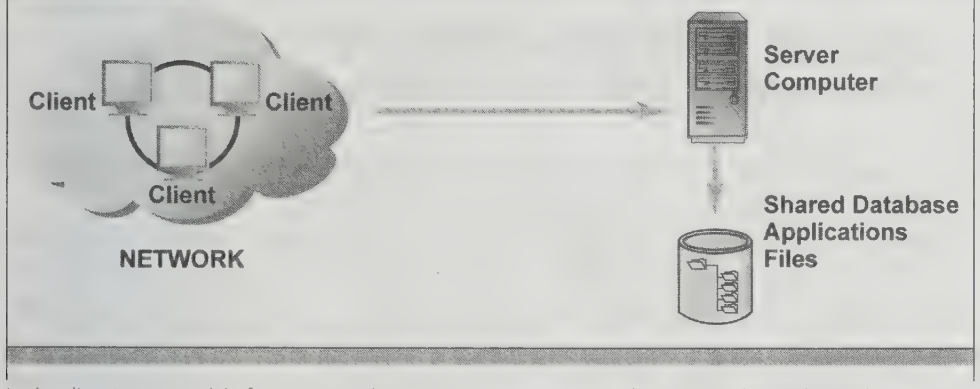
(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and

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

Last modified on October 30, 1995.

SOURCE: Federal Network Council, 1995.

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.

capacity to support graphics or color in text documents, let alone sound files or hyperlinked documents and databases.

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, 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.

Today there are over 1 billion personal computers in existence worldwide (Forrester Research, 2007). Personal computing capabilities are also moving to handheld devices such as BlackBerries, Palms, HP iPAQ Pocket PCs, and cell phones such as Apple's iPhone (much "thinner clients"). In the process, more computer processing will be performed by central servers (reminiscent of mainframe computers of the past). Read *Insight on Business: Peer-to Peer-Networks Rescue Hollywood and TV Studios* for a discussion of a new form of computing that does not directly involve central servers.

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 are services that have been developed over many years and made available to all Internet users.

Pathping
combines the functionality offered by Ping and Tracert

The **Pathping** utility combines the functionality offered by Ping and Tracert. Pathping provides the details of the path between two hosts and statistics for each node in the path based on samples taken over period of time, depending on the number of nodes between the start and end host.

1.3 THE INTERNET TODAY

In 2007, there were an estimated 1.2 billion Internet users worldwide, up from 100 million users at year-end 1997. While this is a huge number, it represents only about 17% of the world's population. That figure is projected to continue to grow to over 1.3 billion by 2008 (Internetworldstats.com, 2007). Internet user growth has slowed in the United States to about 3% annually, but in Asia, Internet growth is about 12% annually. One would think that with such incredible growth worldwide, the Internet would be overloaded. 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.

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

Network Service Provider (NSP)
owns and controls one of the major networks comprising the Internet's backbone

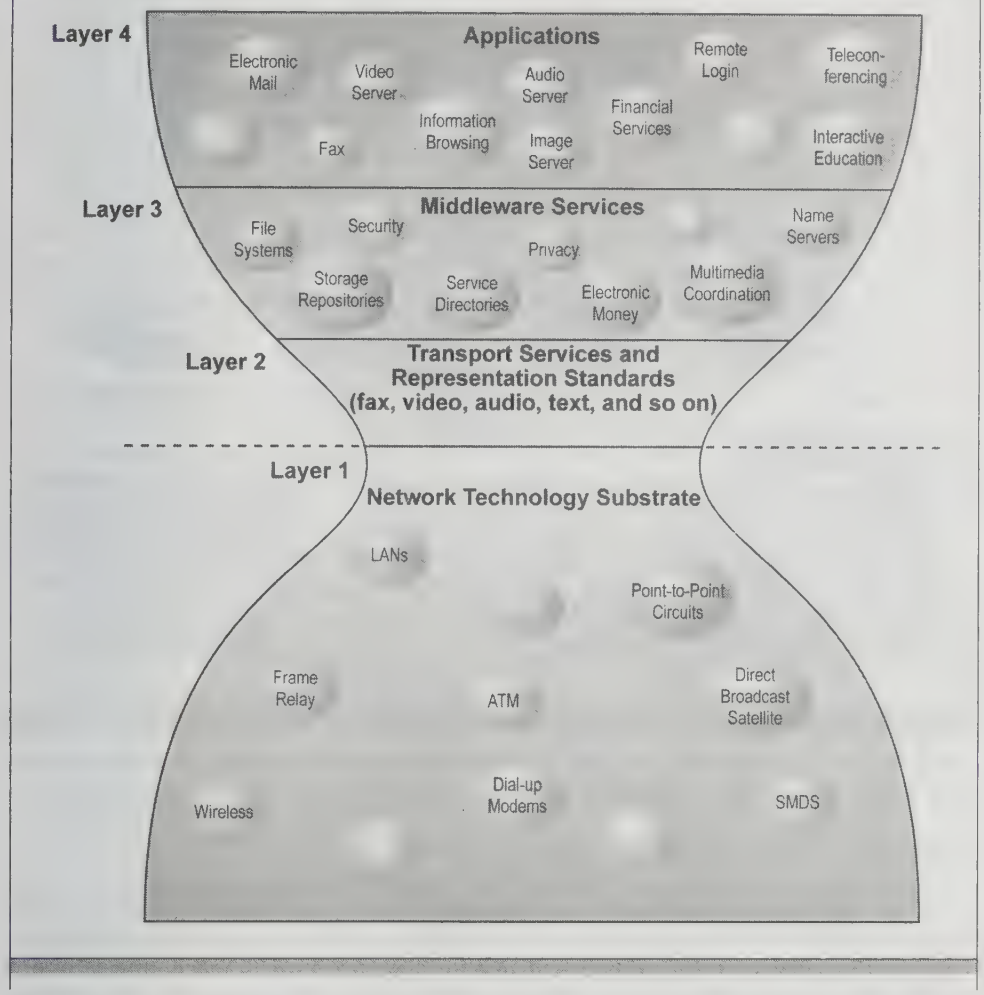
Figure 3.10 illustrates the "hourglass" and layered architecture of the Internet. The Internet can be viewed conceptually as having four layers: the Network Technology Substrate, Transport Services and Representation Standards, Middleware Services, and Applications.[4] The **Network Technology Substrate 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 World Wide 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 changes in the network layer without forcing changes in the applications layer. The Network Technology Substrate layer is further described below.

THE INTERNET BACKBONE

Figure 3.11 illustrates some of the main physical elements of today's Internet. Originally, the Internet had a single backbone, but today's Internet has several backbones that are physically connected with each other and which transfer information from one private network to another. These private networks are referred to as **Network Service Providers (NSPs)**, which own and control the major

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

FIGURE 3.10 THE HOURGLASS MODEL OF THE INTERNET



The Internet can be characterized as an hour-glass 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.

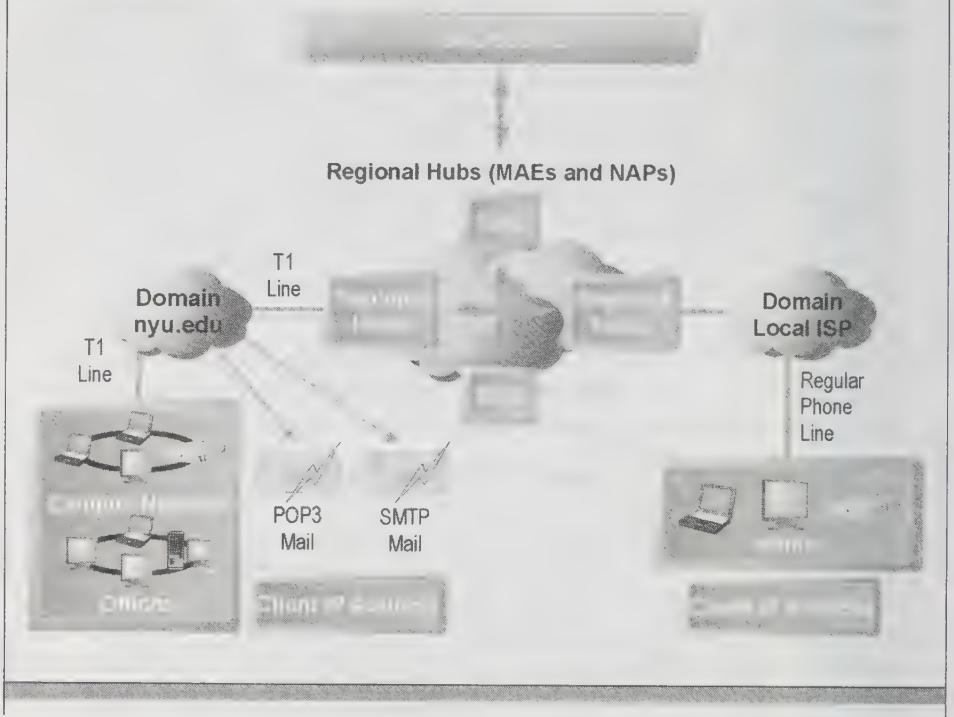
SOURCE: Adapted from Computer Science and Telecommunications Board (CSTB), 2000.

backbone networks (see **Table 3.3**). For the sake of clarity 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)

FIGURE 3.11 INTERNET I NETWORK ARCHITECTURE



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

Connections to other continents are made via a combination of undersea fiber-optic cable and satellite links. The backbones in foreign countries typically are operated by a mixture of private and public owners. The U.S. backbone is one of the most developed because the Internet's infrastructure was developed here. 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.

redundancy
multiple duplicate devices and paths in a network

TABLE 3.3 MAJOR U.S INTERNET BACKBONE OWNERS

AT&T	NTT/Verio
AOL Transit Data Network (ATDN)	Qwest
Cable & Wireless	Sprint
Global Crossing	Verizon
Level 3	

INTERNET EXCHANGE POINTS

In the United States, there are a number of hubs where the backbone intersects with regional and local networks, and where the backbone owners connect with one another (see **Figure 3.12**). 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)**. IXPs use high-speed switching computers to connect the backbone to regional and local networks, and exchange messages with one another. The regional and local networks are owned by local Bell operating companies (RBOCs—pronounced "ree-bocks"), and private telecommunications firms; they generally are fiber-optic networks operating at over 100 Mbps. The regional networks lease access to ISPs, private companies, and government institutions.

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

CAMPUS AREA NETWORKS

Campus 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. 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 2000/2003, Novell NetWare, 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.

campus 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

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 called **Internet Service Providers (ISPs)**. ISPs are retail providers—they deal with "the last mile of service" to the curb—homes and business offices. About 78 million U.S. households connect to the Internet through either a local or national ISP (eMarketer, Inc., 2007a, c). ISPs typically connect to IXPs with high-speed telephone or cable lines (45 Mbps and higher).

There are a number of major ISPs, such as AOL, Earthlink, MSN Network, AT&T WorldNet, Comcast (Optimum Online), Verizon, Sprint, and about 3,500 local ISPs in the United States, ranging from local telephone companies offering dial-up and DSL telephone access to cable companies offering cable modem service, to small "mom-and-pop" Internet shops that service a small town, city, or even county with mostly dial-up phone access. If you have home or small business Internet access, an ISP likely provides the service to you. Satellite firms also offer Internet access, especially in remote areas where broadband service is not available, but satellite firms have had a difficult time penetrating the ISP market because they can offer high-speed download service but they require a telephone service for uplink.

Internet Service Provider (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

Table 3.4 on page 143 summarizes the variety of services, speeds, and costs of ISP Internet connections. There are two types of ISP service: narrowband and broadband.

SOME MAJOR U.S. INTERNET EXCHANGE POINTS (IXPs)

Region	Name	Location	Operator
EAST	MAE East	Virginia and Miami	MCI
	New York International Internet Exchange (NYIIX)	New York	Telehouse
	Peering and Internet Exchange (PAIX)	New York, Philadelphia and Northern Virginia	Switch and Data
	NAP of the Americas	Miami	Terramark
CENTRAL	MAE Chicago	Chicago	MCI
	Chicago NAP	Chicago	SBC
	MAE Central	Dallas and Atlanta	MCI
	Peering and Internet Exchange (PAIX)	Atlanta	Switch and Data
WEST	MAE West	San Jose and Los Angeles	MCI
	Peering and Internet Exchange (PAIX)	Palo Alto, San Jose, and Seattle	Switch and Data
	Los Angeles International Internet Exchange (LAIIX)	Los Angeles	Telehouse

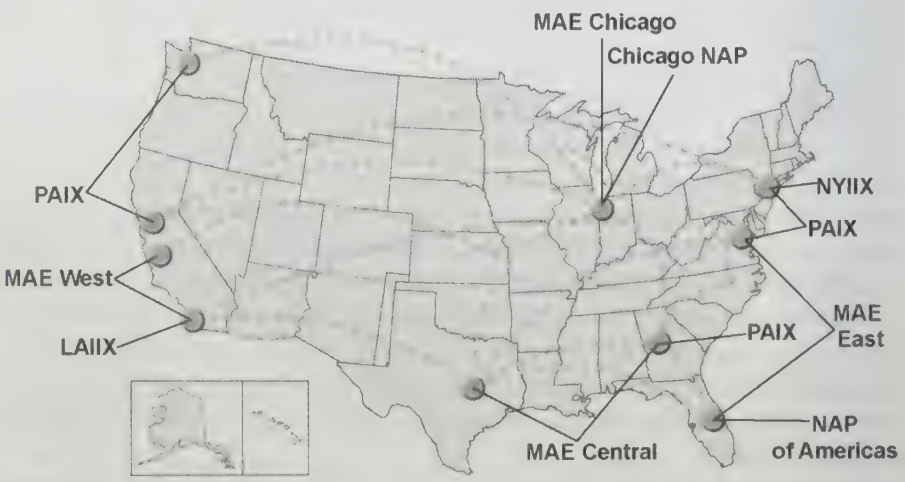


TABLE 5.1 ISP SERVICE LEVELS AND BANDWIDTH CHOICES

SERVICE	COST/MONTH	SPEED TO DESKTOP (KBPS)
Telephone modem	$10–$25	30–56 Kbps
DSL	$15–$50	1 Mbps–3 Mbps
Cable modem	$20–$50	1 Mbps–15 Mbps
Satellite	$20–$50	250 Kbps–1 Mbps
T1	$1,000–$2,000	1.54 Mbps
T3	$10,000–$30,000	45 Mbps

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 is quickly being replaced by broadband connections in the United States, Europe, and Asia. Broadband service is based on DSL, cable modem, 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—generally anything above 100 Kbps. In the United States, broadband users surpassed dial-up users in 2004, and in 2007 there were 65 million broadband households and 22 million dial-up households (eMarketer, Inc., 2007a).

The actual throughput of data will depend on a variety of factors including noise in the line and the number of subscribers requesting service. T1 lines are publicly regulated utility lines that offer a guaranteed level of service, but the actual throughput of the other forms of Internet service is not guaranteed.

Digital Subscriber Line (DSL) service is a telephone technology for delivering high-speed access to the Internet through ordinary telephone lines found in a home or business. Service levels range from about 768 Kbps all the way up to 3 Mbps. DSL service requires that customers live within two miles (about 4,000 meters) of a neighborhood telephone switching center.

Cable modem 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. Cable modem services range from 1 Mbps up to 15 Mbps. Comcast, Time Warner Road Runner, and Cox are the largest 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 delivery at a whopping 45 Mbps. T1 lines cost about $1,000–$2,000 per month, and **T3** lines between $10,000 and $30,000 per month. These are leased, dedicated, guaranteed lines suitable for corporations, government agencies, and businesses such as ISPs requiring high-speed guaranteed service levels.

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—generally anything above 100 Kbps

Digital Subscriber Line (DSL)
a telephone technology for delivering high-speed access through ordinary telephone lines found in homes or businesses

cable modem
a cable television technology that 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

Some satellite companies offer broadband high-speed digital downloading of Internet content to homes and offices that deploy 18" satellite antennas. Service is available beginning at 256 Kbps up to 1 Mbps. In general, satellite connections are not viable for homes and small businesses because they are only one-way—you can download from the Internet at high speed, but cannot upload to the Internet at all. Instead, users need a phone or cable connection to upload.

Prices are falling drastically to as low as $14.95 per month for DSL service. Cable broadband accounts for nearly 60% of all broadband users and nearly all large business firms and government agencies have broadband connections to the Internet. Demand for broadband service has grown so rapidly simply because it greatly speeds up the process of downloading Web pages and increasingly large video and audio files located on Web pages (see **Table 3.5**). As the quality of Internet service offerings expands to include Hollywood movies, music, games, and other rich media-streaming content, the demand for broadband access will continue to swell.

INTRANETS AND EXTRANETS

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

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 providers of local area network software are Microsoft's Windows 2000/2003 server software, followed by open source Linux, both of which use TCP/IP networking protocols.

TABLE 3.5 TIME TO DOWNLOAD A 10-MEGABYTE FILE BY TYPE OF INTERNET SERVICE

TYPE OF INTERNET SERVICE	TIME TO DOWNLOAD
NARROWBAND SERVICES	
Telephone modem	25 minutes
BROADBAND SERVICES	
DSL @ 1 Mbps	1.33 minutes
Cable modem @ 10 Mbps	8 seconds
T1	52 seconds
T3	2 seconds

Extranets are formed when firms permit outsiders to access their internal TCP/IP networks. For instance, General Motors permits parts suppliers to gain access to GM's intranet that contains GM's production schedules. In this way, parts suppliers know exactly when GM needs parts, and where and when to deliver them.

extranet
formed when firms permit outsiders to access their internal TCP/IP networks

Intranets and extranets generally do not involve commercial transactions in a marketplace, and they are mostly beyond the scope of this text. Extranets will receive some attention as a technology that supports certain types of B2B exchanges (described in Chapter 12).

WHO GOVERNS THE INTERNET?

Aficionados and promoters of the Internet 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 which 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 legislatures, and international professional societies. There is no one governing organization that controls activity on the Internet. Instead, there are several organizations that influence the system and monitor its operations. Among the governing bodies of the Internet are:

- The *Internet Architecture Board (IAB)*, which helps define the overall structure of the Internet.
- The *Internet Corporation for Assigned Names and Numbers (ICANN)*, which assigns IP addresses, and the *Internet Network Information Center (InterNIC)*, which assigns domain names. ICANN was created in 1998 by the U.S. Department of Commerce to eventually take over the domain name system and the 13 root servers that are at the heart of the Internet addressing scheme.
- The *Internet Engineering Steering Group (IESG)*, which oversees standard setting with respect to the Internet.
- The *Internet Engineering Task Force (IETF)*, a private-sector group which forecasts the next step in the growth of the Internet, keeping watch over its evolution and operation.
- The *Internet Society (ISOC)*, which is a consortium of corporations, government agencies, and nonprofit organizations that monitors Internet policies and practices.
- The *World Wide Web Consortium (W3C)*, a largely academic group that sets HTML and other programming standards for the Web.
- The *International Telecommunication Union (ITU)*, which helps set technical standards.

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.

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 the nation-state. Although in the early years of the Internet and the Web 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.

While, as noted previously, the U.S. Department of Commerce originally created ICANN with the intent that it take over control of the Domain Name System, this is no longer the case. The United States changed its policy in June 2005, when the Department of Commerce announced it would retain oversight over the 13 root servers which serve as master directories for Web browsers and e-mail programs throughout the world. Observers give 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. Countries who refuse to accept U.S. control over the Internet could set up their own separate domain name systems, fracturing today's single Web into many different, potentially incompatible networks. A United Nations panel set up to devise a global plan for the Internet has failed to come to an agreement. The Working Group on Internet Governance (WGIG) decided instead to set up a permanent forum to carry on the debate and issued an interim report in June 2005, calling for international governance of the Internet. There have been no further meetings of WGIG.

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

3.3 INTERNET II: THE FUTURE INFRASTRUCTURE

The Internet is changing as new technologies appear and new applications are developed. We refer to the future infrastructure as Internet II. The second era of the Internet is being built today by private corporations, universities, and government agencies. To appreciate the benefits of Internet II, 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

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

database server
server designed to access specific information with 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

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.

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 computer, with various flavors of Unix/Linux computers a distant third. However, the fastest-growing category of Web clients are not computers at all, but cell phones and handheld PDAs outfitted with wireless Web access software. In general, Web clients can be any device—including a refrigerator, stove, home lighting system, or automobile instrument panel—capable of sending and receiving information from Web servers.

WEB BROWSERS

Web browsers are software programs 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). The leading Web browsers are Internet Explorer, with about 75% of the market as of June 2007. Firefox (Mozilla) is currently the second most popular Web browser, with about 20% of the U.S. Web browser market (eMarketer, 2007d). First released in 2004, Firefox is a free, open source Web browser for the Windows, Linux and Macintosh operating systems, based on Mozilla open source code (which originally provided the code for Netscape). It is small and fast and offers many new features such as pop-up blocking and tabbed browsing. Other browsers include Apple's Safari, Opera, and Netscape Navigator, which collectively make up 5% of the market.

3.3 THE INTERNET AND THE WEB: FEATURES

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

The Internet and the Web have spawned a number of powerful new software applications upon which the foundations of e-commerce are built. You can think of these all 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 how rich is the Internet environment.

E-MAIL

Since its earliest days, **electronic mail**, or **e-mail**, has been the most-used application of the Internet. In the United States about 80 million people send e-mail every

day, and worldwide over 600 million send e-mail daily. The total number of e-mail messages (including commercial, personal, and spam) sent daily in the United States in 2007 is estimated to be around 31 billion (1 trillion per year) (Evert, 2007; eMarketer, Inc., 2007e). Estimates vary on the amount of spam, ranging from 40% to 90%, with a notable spike towards the higher number beginning in the latter part of 2006. E-mail marketing and spam are examined in more depth in Chapter 7.

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

attachment
a file inserted within an e-mail message

INSTANT MESSAGING

One of the fastest growing forms of online human communication is **instant messaging (IM)**. An instant messenger is a client software program that signs onto an instant messaging server. IM sends text messages in real time, one line at a time, unlike e-mail. E-mail messages have a time lag of several seconds to minutes between when messages are sent and received. IM displays lines of text entered on a computer 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 identify 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, users can insert audio clips or photos into their instant messages, and even participate in video conferencing.

instant messaging (IM)
displays words typed on a computer 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

The major IM systems are AOL (which first introduced IM as a proprietary consumer service in 1997), with around 44.5 million unique users; Microsoft's Windows Live Messenger, with about 26 million; Yahoo Messenger, with about 22 million; and Google Talk with 1.7 million. IM systems were initially developed as proprietary systems, with competing firms offering versions that did not work with one another. However, in 2006, Yahoo and MSN joined together to provide a level of interoperability between their respective systems, and Google has announced talks with AOL to do the same (Perez, 2007).

SEARCH ENGINES

No one knows for sure how many Web pages there really are. The surface Web is that part of the Web which search engines visit and record information about. For instance, Google currently searches about 50 billion Web pages and stores information about those pages in its massive computer network located throughout the United States. Microsoft and Yahoo presumably index a similar number of pages, AskJeeves is estimated to index 10 billion pages. But there is also a "deep Web" that contains an estimated 900 billion additional Web pages, many of them proprietary (such as the pages of the online version of *The Wall Street Journal*, which

cannot be visited without an access code) or behind corporate firewalls (Zillman, 2005).

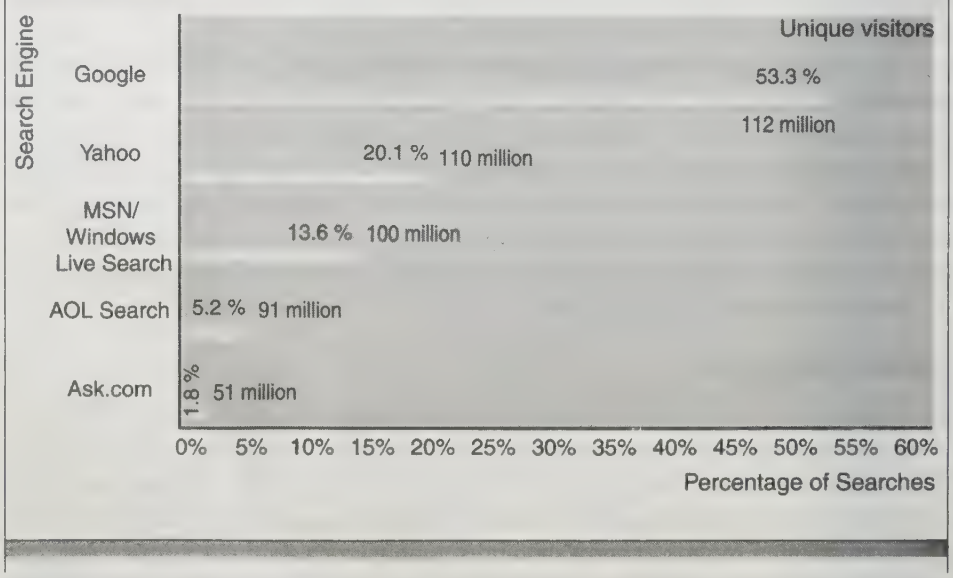
But obviously with so many Web pages, finding Web specific pages that can help you or your business, nearly instantly, is an important problem. The question is: how can you find the one or two Web pages you really want and need out of the 50 billion indexed Web pages?

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

Search engines solve the problem of finding useful information on the Web nearly instantly, and, arguably, they are the "killer app" of the Internet era. About 40 million Americans use search engines each day, generating about 7.5 to 8 billion queries a month (Pew Internet & American Life Project, 2007a, Nielsen/NetRatings, 2007). There are hundreds of different search engines in the world, but the vast majority of the search results are supplied by the top five providers (see **Figure 3.20**).

Web search engines started out in the early 1990s shortly after Netscape released the first commercial Web browser. Early browsers 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 + search engine".

FIGURE 3.20 TOP FIVE SEARCH ENGINES



Google is, by far, the leading search engine based on its percentage share of the number of searches. In terms of unique visitors, however, the top three sites are much more tightly bunched.

SOURCE: Based on data from Nielsen/NetRatings, 2007a, 2007b; Burns, 2007; Kee, 2007.

The Google search engine is continuously crawling the Web, indexing the content of each page, calculating its popularity, and caching the pages so that it can respond quickly to your request to see a page. The entire process takes about one-half of a second.

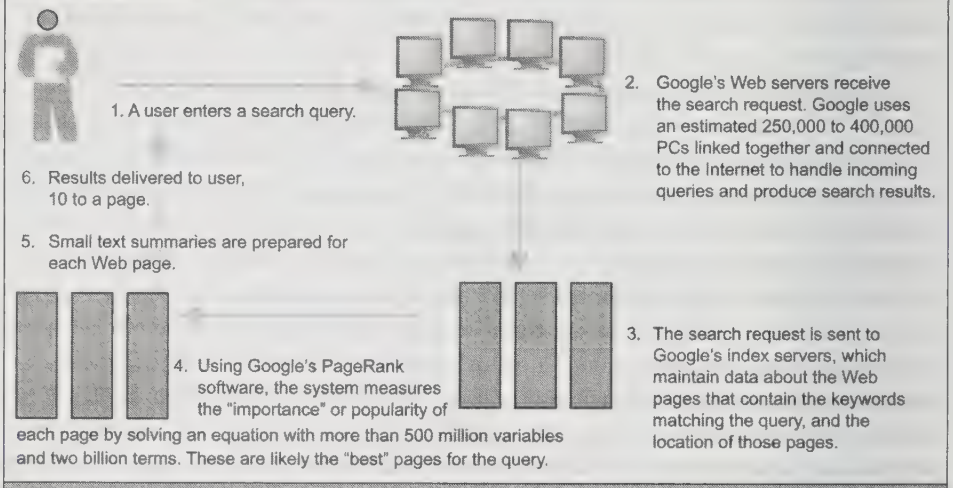
The first search engines employed simple keyword indexes of all the Web pages visited. They would count the number of times a word appeared on the Web page, and store this information in an index. These search engines could be easily fooled by Web designers who simply repeated words on their home pages. The real innovations in search engine development occurred through a program funded by the Department of Defense called the Digital Library Initiative, designed to help the Pentagon find research papers in large databases. Stanford, Berkeley, and three other universities became hotbeds of Web search innovations in the mid-1990s. At Stanford in 1994, two computer science students, David Filo and Jerry Lang, created a hand-selected list of their favorite Web pages and called it "Yet Another Hierarchical Officious Oracle" or Yahoo!. Yahoo initially was not a real search engine, but rather an edited selection of Web sites organized by categories the editors found useful. Yahoo has since developed "true" search engine capabilities.

In 1998, Larry Page and Sergey Brin, two Stanford computer science students, released their first version of Google. 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 3.21** illustrates how Google works.

Search engine Web sites have became so popular and easy to use that they also serve as major portals for the Internet (see Chapter 11). The search marketplace has become very competitive despite the dominance of Google. Both Microsoft and Yahoo have invested over a billion dollars each to match Google's search engine.

Initially, few understood how to make money out of 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 over the last few years at around 20%–25% annually), has helped search engines transform themselves into major shopping tools and created an entire new industry called "search engine marketing." Search engine marketing has been the fastest-growing form of advertising in the United States, reaching about $10 billion in 2007. When users enter a search term at Google, MSN

FIGURE 3.21 HOW GOOGLE WORKS



The Google search engine is continuously crawling the Web, indexing the content of each page, calculating its popularity, and caching the pages so that it can respond quickly to your request to see a page. The entire process takes about one-half of a second.

Search, Yahoo, or any of the other Web sites 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. In addition, advertisers can purchase small text ads on the right side of the search results page. 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 Web sites, the search engine is limited to finding matches from that one site. In addition, search engines are extending their services to include maps, satellite images, computer images, e-mail, group calendars, group meeting tools, and indexes of scholarly papers. Outside of e-mail, search engines are the most common online daily activity and produce the largest online audiences.

INTELLIGENT AGENTS (BOTS)

intelligent agent software program that gathers and/or filters information on a specific topic and then provides a list of results for the user

An **intelligent agent** (also known as a software robot, or bot, for short) is a software program that gathers and/or filters information on a specific topic, and then provides a list of results for the user ranked in a number of ways, such as from lowest price to availability or to delivery terms. Intelligent agents were originally invented by computer scientists interested in the development of artificial intelligence (a family of related technologies that attempt to imbue computers with human-like intelligence). However, with the advent of e-commerce on the Web, interest quickly turned to exploiting intelligent agent technology for commercial purposes. Today, there are a number of different types of bots used in e-commerce on the Web, and

TABLE 3.12 TYPES OF WEB BOTS

TYPE	EXAMPLES
Search bot	Searchbot.com Altavista.com Webcrawler.com
Shopping Bot	Shopzilla.com Shopping.com MySimon.com Orbitz.com
Web Monitoring Bot	WebSite Watcher TimelyWeb.com
News Bot	WebClipping.com SportSpider.net
Chatter Bot	Anna (Ikea) Ask Vic (Qantas) Virtual Advisor (Ultralase)

more are being developed every day (see **Table 3.12**).

For instance, as previously noted, many search engines employ Web crawlers or spiders that crawl from server to server, compiling lists of URLs that form the database for the search engine. These Web crawlers and spiders are actually bots, automated programs that search the Web for a variety of reasons.

The shopping bot is another common type of bot. Shopping bots search online retail sites all over the Web and then report back on the availability and pricing of a range of products. For instance, you can use MySimon's shopping bot to search for a Sony digital camera. The bot provides a list of online retailers that carry a particular camera model, as well as report about whether it is in inventory and the price and shipping charges. Orbitz provides bots that find the lowest prices for airfares, hotels, and rental cars. Shopping.com is the leading comparison shopping Web site with an estimated 20.5 million unique monthly visitors in 2007, followed by Shopzilla.com, with an estimated 16 million, and Yahoo Shopping with an estimated 14 million. About 60% of consumers have used a comparison shopping Web site.The number of shoppers visiting such sites is also growing rapidly at about 15% annually (Internet Retailer, 2007).

Another type of bot, called a Web monitoring bot, allows you to monitor for updated materials on the Web, and will e-mail you when a selected site has new or changed information. News bots will create custom newspapers or clip articles for you in newspapers around the world. RSS (Really Simple Syndication), discussed later in this chapter, is also a kind of automated program that sends updates and news to subscribers, and is quickly becoming the most common type of Web content monitoring tool.

Read *Insight on Technology: Chatterbots Meet Avatars*, to see how a bot with academic roots has morphed into an e-commerce customer-support tool.

INSIGHT ON TECHNOLOGY

CHATTERBOTS MEET AVATARS

In the early 1960s, Joseph Weizenbaum, a professor of computer science at the Massachusetts Institute of Technology, created a software program known as Eliza. Eliza was one of the first software programs to allow a computer to "converse" with a human in natural language. Weizenbaum programmed Eliza so that it was able to recognize certain key words in a statement or question. Eliza would then respond based on a set of preprogrammed rules. Sometimes Eliza was able to carry on a passable conversation—for a short period of time. More often than not, though, the conversation quickly degenerated into something no person would mistake for a human interaction. The trick behind Eliza was to answer a human's statements and questions with reasonable-sounding but ultimately meaningless questions drawn from Rogerian psychotherapy that were intended to encourage the patient to talk more about themselves.

From this rudimentary beginning in computer science departments sprang chatterbots: commercial-quality intelligent agents (computer programs) that could converse with a customer over the telephone or the Web either in text or voice modes. Sometimes called "virtual reps" or "remote agents," later chatterbots were programmed to both recognize human speech and to respond with meaningful suggestions or questions. Chatterbots are viewed as one possible answer to the customer service difficulties plaguing many e-commerce sites, problems that will cost e-tailers billions of dollars in 2007. For instance, one study found that the response times of Fortune 100 companies to simple e-mail queries left much to be desired, with only 13% responding within 24 hours; 37% of Fortune 500 companies did not respond to general inquiries submitted to their Web sites at all. Another study found that over 65% of those who start to fill up a shopping cart abandon it before going through the check-out process, for a variety of reasons, including poor Web site design, a confusing check-out process, or questions that were unanswered.

If you call a large bank, credit card provider, or your cell service provider, chances are good you will be encouraged to talk with a chatterbot. They are on duty 24/7, cost very little to operate, and can answer many questions of consumers using natural language interfaces and synthesized voices. No one knows for sure, but millions of transactions in the United States and Europe are handled by chatterbots every day. One of the largest commercial providers of virtual reps is the U.K firm Creativevirtual.com. They supply virtual online sales reps to BP, Lloyds, Sky.com, and Schering-Plough. Ikea's "Anna" is available on Ikea's Web sites worldwide in several different languages and acts as a guide to customers who land on the Ikea home page and don't have a clue about where to go next.

The problem with chatterbots is that they are not human, just computer programs with funny voices. Avatars may be an alternative. Increasingly, chatterbots are taking on the characteristics of 3-D Second Life avatars, or let's say the two are merging, or is it marrying?

An avatar is a computer-based representations of a person, usually as an animated graphic. They are created using a variety of different programs, and once created, they can be used in computer games, on instant messaging services, blogs, or in virtual communities such as Second Life, an "online 3-D digital world" that is

(continued)

"home" to 8 million Internet users. Avatars, unlike chatterbots, use the mind of their creators when interacting with other avatars as opposed to a computer program, and they express themselves using text, or online voice using VoIP. Avatars can be recorded on video, and the video played back.

Firms are beginning to experiment with virtual business centers on Second Life. A virtual business center is a location on Second Life where a firm can construct a building or office space, and where it can display its products and services to other avatars who come visit. For instance, IBM has set up a virtual business center staffed by IBM sales representatives from around the world. Clients who want buy or shop for hardware, software, or services can get help from IBM avatars who, in reality, are live IBM sales reps. The avatars can handle all aspects of customer requests up to the actual money transaction, sharing of credit information, or signing legal documents. Those aspects of the sales transaction are transferred to real people. The IBM sales reps' avatars are available in English, Portuguese, German, Spanish, Dutch, Italian, and French.

Reebok, Adidas, American Apparel, and 1-800-Flowers are also setting up shop on Second Life using avatars to present their products. At Reebok, users can create and buy tennis shoes for their avatars, and go to Reebok.com and purchase real-world tennis shoes for themselves. 1-800-Flowers sells both virtual bouquets and directs users to the real-world site for people bouquets.

So why should a business invest in avatars? Some possibilities include using avatars to place and time shift, for instance, by creating a presence at a trade show without actually traveling there, or by creating sales demonstrations of products, recording them, and playing them back to visiting avatars.

At this point, the commercial uses of avatars are just being explored. But as thousands of businesses join digital environments such as Second Life, avatars will play a growing role in remote sales and service. The problem with avatars is that there's an expensive human behind the pretty graphics. One solution might be to add a little artificial intelligence to the avatar's front end. Whether or not humans will be fooled by this artifice is not known.

SOURCES: "'That Looks Great on You': Online Sales People Get Pushy," *Wall Street Journal*, January 3, 2007; "In 3-D Virtual World, Business Never Sleeps," by Dwight Adams, *Indianapolis Star*, June 25, 2007;" Awaiting Real Sales From Virtual Shoppers," by Bob Tedeschi, *New York Times*, June 11, 2007; "IBM Opens Sales Center in Second Life," by Jon Brodkin, *Networkworld*, May 15, 2007; "Chatterbots," by Jill Ruchala, *New York Press*, August 17, 2005.

ONLINE FORUMS AND CHAT

An **online forum** (also referred to as a message board, 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 forum provides a container for various discussions (or "threads") started (or "posted") by members of the forum, and depending on the permissions granted to forum members by the forum's administrator, enables a person to start a thread and reply to other people's threads. Most forum software allows more than one forum to be created. The forum administrator typically can edit, delete, move, or otherwise modify any thread on the forum. Unlike an electronic mailing list (such as a listserv), which automatically sends new messages to a subscriber, an online forum

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

typically requires that the member visit the forum to check for new posts. Some forums offer an "e-mail notification" feature that notifies users that a new post of interest to them has been made.

online chat
enables users to communicate via computer in real time, that is, simultaneously. Unlike IM, chat can occur among several users

Online chat differs from an online forum in that, like IM, chat enables users to communicate via computer in real time, that is, simultaneously. However, unlike IM, which works only between two people, chat can occur among several users. Typically, users log in to a "chat room" where they can text message others. Some chat rooms offer virtual chat, which enable users to incorporate 2-D and 3-D graphics along with avatars (an icon or representation of the user) into their chat, or offer the ability to communicate via audio and/or video. Chat systems include Internet Relay Chat (IRC), Jabber, and a number of proprietary systems based on the Microsoft Windows or Java platform. E-commerce firms typically use online forums and online chat to help develop community and as customer service tools. We will discuss the use of online forums as a community-building tool further in Chapter 11.

STREAMING MEDIA

streaming media
enables music, video, and other large files to be sent to users in chunks so that when received and played, the file comes through uninterrupted

Streaming media enables live Web video, music, video, and other large bandwidth files to be sent to users in a variety of ways that enable the user to play back the files. In some situations, such as live Web video, the files are broken into chunks and served by specialized video servers to users in chunks. Client software puts the chunks together and plays the video. In other situations, such as YouTube, a single large file is downloaded from a standard Web server to users who can begin playing the video before the entire file is downloaded. Streamed files must be viewed "live": they cannot be stored on client hard drives. Streamed files are "played" by a software program such as Microsoft's Media Player, Apple QuickTime, Flash, and RealMedia Player. There are a number of tools used to create streaming files but one of the most common is Adobe's Flash program. The Flash player has the advantage of being built into most client browsers; no plug-in is required to play Flash files.

Sites such as YouTube, MetaCafe, and GoogleVideo have popularized user-generated video streaming. Web advertisers increasingly use video to attract viewers. Streaming audio and video segments used in Web ads and news stories are perhaps the most frequently used streaming services. As the capacity of the Internet grows, streaming media will play an even larger role in e-commerce.

cookie
a tool used by Web sites to store information about a user. When a visitor enters a Web site, the site sends a small text file (the cookie) to the user's computer so that information from the site can be loaded more quickly on future visits. The cookie can contain any information desired by the site designers

COOKIES

A **cookie** is a tool used by a Web site to store information about a user. When a visitor enters a Web site, the site sends a small text file (the cookie) to the user's computer so that information from the site can be loaded more quickly on future visits. The cookie can contain any information desired by the Web site designers, including customer number, pages visited, products examined, and other detailed information about the behavior of the consumer at the site. Cookies are useful to consumers because the Web site will recognize returning patrons and not ask them to register again. Cookies are also used by advertisers to ensure visitors do not receive the same advertisements repeatedly. Cookies can also help personalize a Web site by allowing the site to recognize returning customers and make special offers to them based on

their past behavior at the site. Cookies allow Web marketers to customize products and segment markets—the ability to change the product or the price based on prior consumer information (described more fully in later chapters). As we will discuss throughout the book, cookies also can pose a threat to consumer privacy, and at times they are bothersome. Many people clear their cookies at the end of every day. Some disable them entirely using tools built into most browsers.

NEW AND DISRUPTIVE WEB FEATURES AND SERVICES

Today's broadband Internet infrastructure has greatly expanded the services available to users. These new capabilities have formed the basis for new business models. Digital content and digital communications are the two areas where innovation is most rapid.

Blogs (Weblogs)

There are so many "killer apps" on the Web that it's hard to pick one super app. But blogs arguably are a super app. A **blog**, or **weblog**, is a personal Web page that typically contains a series of chronological entries (newest to oldest) by its author, and links to related Web pages. The blog may include a blogroll (a collection of links to other blogs) and TrackBacks (a list of entries in other blogs that refer to a post on the first blog). Most blogs allow readers to post comments on the blog entries as well. The act of creating a blog is often referred to as "blogging." Blogs are either hosted by a third-party site such as Blogger.com (owned by Google), LiveJournal, Typepad, Xanga, or Wordpress, or prospective bloggers can download software such as Moveable Type and bBlog 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 Web sites is often referred to as the blogoshpere.

weblog (blog)
personal Web page that is created by an individual or corporation to communicate with readers

The content of blogs range from individual musings to corporate communications. Blogs have had a significant impact on political affairs, and have gained increasing notice for their role in breaking and shaping the news. Blogs have become hugely popular. While estimates on the number of blogs vary, Technorati, a weblog research firm, claims there were over 105 million blogs as of September 2007, with 175,000 created each day, and 1.6 million postings (Technorati, 2007). No one knows how many of these blogs are kept up to date or just yesterday's news. And no one knows how many of these blogs have a readership greater than one (the blog author). Other, perhaps more reliable surveys find about 11 million people have created a blog, and 55 million read blogs regularly in the United States (Pew Internet, 2007b). In fact, there are so many blogs you need a blog search engine just to find them (such as Google's search engine), or you can just go to a list of the most popular 100 blogs and dig in. We discuss blogs further in Chapter 6 as a marketing mechanism, and in Chapter 10 as one part of the significant growth in user-generated content enabled by the Internet.

CHAPTER 5

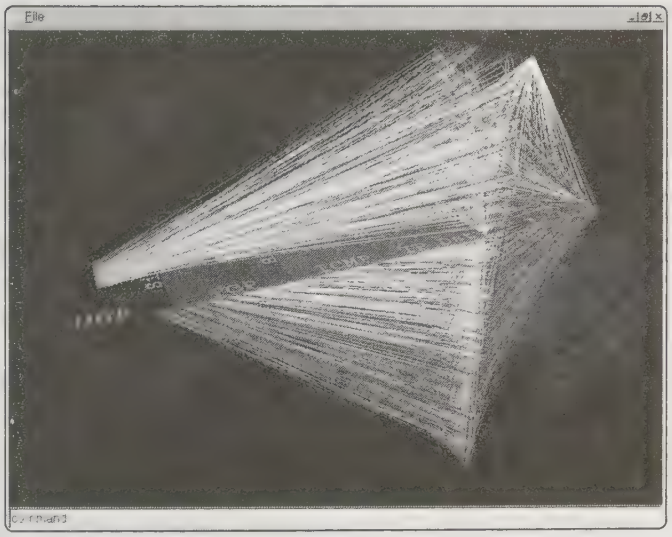
Online Security and Payment Systems

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

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

Cyberwar in Estonia



A computer-generated simulation of a DDoS attack.

Estonia is a very small country with a little more than 1 million citizens in northeastern Europe, bounded by Russia to the east, the Gulf of Finland to the north, and the Baltic Sea and Sweden to the west. Despite its small size, it was the location of a momentous Internet security event on April 26, 2007—perhaps the most significant Internet security event in history, in terms of size, scale, and sheer chutzpah. It all started in early April 2007, when the Estonian government began dismantling a bronze statue of a World War II-era Soviet soldier, and began moving the statue from its previous location in a park to a suburban cemetery. Ethnic Russians took to the streets in protest, but by April 29, the streets of capital city Tallinn were calm. Estonia's Internet infrastructure, however, was under attack.

Beginning on April 26, the Internet addresses of the Estonian government and some Estonian banks began to receive the first trickle of requests for service from an unusual number of foreign Internet addresses, some identified as Russian government sites located inside the Kremlin, and a part of Russian premier Vladimir Putin's administration. Within hours, on April 27, the trickle became a flood of highly distributed requests from millions of computers worldwide. It was the beginning of a massive, unparalleled Distributed Denial of Service (DDoS) attack launched by a global network of so-called zombie computers linked together in a botnet.

Attackers began with a trickle of requests to identify Estonian servers, and then sent a huge burst of data to measure the capacity of the network. Once the throughput capacity of the network was estimated, the attackers contracted with botnet operators worldwide, and used botnets under their own control, to initiate a sustained multi-week attack on the Estonian servers. In ten large assaults, over 1 million computers worldwide slammed the Estonia servers with junk messages and requests, producing streams of 90 megabits of data a second for ten hours, far beyond the capacity of Estonia's routers, switches, and Web servers.

In Estonia, the Web is a little more important than it is in the United States or Europe. In Estonia, people use the Web to pay for groceries, pay for newspapers using mobile digital wallets, and file their taxes, as well as pay traffic fines. In Estonia, the Web and Internet are a basic utility and infrastructure for the economy. While the Estonian government's software engineers were able to survive the attacks, the Bank of Estonia was forced to shut down and also cut off access to banks outside the country for a period of time. E-mail, purchases, and payments all slowed to a crawl. Government agencies temporarily slowed and closed in some cases.

While cyberwar has been written about in novels, and has been demonstrated on a small scale, the Estonian situation, malicious strikes against Web sites of specific companies (often as part of a blackmail plot), and a major attack against VeriSign illustrate that cyberwar is now a reality on a much scarier scale. In the VeriSign case, several botnets involving several hundred thousand computers around the globe attempted to overwhelm all of the 13 root server systems—the top level domains such as .com, .org, .net, and others. The attack failed but severely stressed the United States Internet infrastructure, slowing down the Internet and demonstrating how fragile the entire system is to such attacks.

Imagine: about 10% of the world's billion computers connected to the Internet worldwide are captured by stealth malware programs that users unintentionally install by opening e-mail attachments or clicking malicious links that download files, or as a result of using pirated "free" software. RustockB is one common stealth program that adds unwitting users to botnets. These programs then take over the computer without the user knowing and are controlled remotely by a Command and Control server. Once under control, the botnet is used to send spam. Botnets are responsible for over 80% of the spam sent throughout the world. This is the most profitable use of botnets. They are also used to collect credit card information, personal IDs, and bank information, feeding the underground economy with identity theft candidates. The botnets can be "rented" to run DDoS attacks against any site on the Internet. It could be your company, or your bank. ShadowServer, an organization of volunteer computer security experts, tracks 400,000 known infected computers (a small fraction of the total) and about 1,500 active controllers.

Today, Estonia is back online. The attacks have leveled off, and ultimately they did not lead to the collapse of the Estonian government, society, or business. VeriSign is tripling the size of its domain name server installation to fend off future attacks. But defense authorities, government agencies, and businesses are unlikely to be able to fend off these attacks forever without some re-design of the Internet itself simply because the scale of the botnets is growing faster than the scale of the defensive moves.

SOURCES: "Net Attack," by Aaron Mannes and James Hendler, *Wall Street Journal*, June 5, 2007; "War Fears Turn Digital After Data Siege in Estonia," by Mark Lander and John Markoff, *New York Times*, May 29, 2007; "VeriSign Moves to Address an Internet Security Problem," by John Markoff, *New York Times*, February 8, 2007; "Attack of the Zombie Computers Is Growing Threat," by John Markoff, *New York Times*, January 7, 2007.

As *Cyberwar in Estonia* 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. However, there are steps you can take to protect your Web sites and your personal information when using online e-commerce sites.

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.

5.1 THE E-COMMERCE SECURITY ENVIRONMENT

For most law-abiding citizens, the Internet holds the promise of a huge, 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 billion consumers in the world on the Internet. 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, on the Internet you can download the same music for free and almost without risk. 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 a billion users, and lacks many basic security features found in older networks such as the telephone system or broadcast television networks. Who ever heard of the telephone system being hacked and "brought down" by programmers in Eastern Europe? 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. However, the overall security environment is strengthening as business managers and government officials make significant investments in security equipment and business procedures.

THE SCOPE OF THE PROBLEM

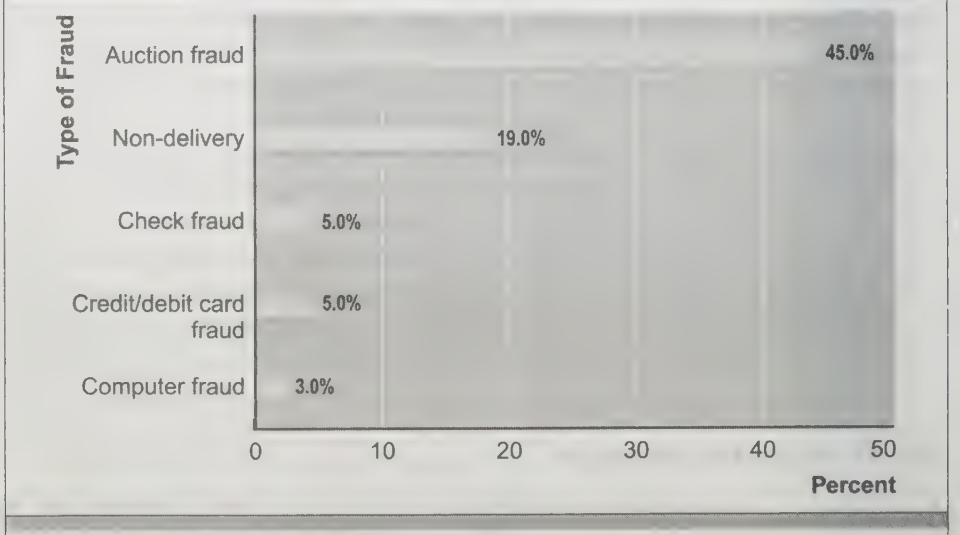
Cybercrime is becoming a more significant problem for both organizations and consumers. Bot networks, DoS, and DDoS attacks (all described in the opening case), Trojans, phishing (fraudulently obtaining financial information from a victim, typically via e-mail), data theft, identity theft, credit card fraud, and spyware are just some of the threats that are making daily headlines. But despite

the increasing attention being paid to cybercrime, it is difficult to accurately estimate the actual amount of such crime, in part because some companies may be hesitant to report crime due to fear of losing the trust of its customers, and because even if crime is reported, it may be difficult to quantify the actual dollar amount of the loss.

One source of information is the Internet Crime Complaint Center ("IC3"), a partnership between the National White Collar Crime Center and the Federal Bureau of Investigation. The IC3 data is useful for gauging the types of e-commerce crimes most likely to be reported by consumers and the typical amount of loss experienced. In 2006, the IC3 processed more than 200,000 Internet crime complaints and referred almost 90,000 of them to federal, state, and local law enforcement agencies. The total dollar loss from all referred cases was almost $200 million, and the average dollar loss was about $2,500. **Figure 5.1** provides a summary of the top 5 categories of reported complaints, and **Figure 5.2** shows the average dollar loss for various categories. Auction fraud was the most frequently reported complaint, while the highest dollar loss per incident arose from Nigerian letter fraud (a form of phishing) (National White Collar Crime Center and the Federal Bureau of Investigation, 2007).

The Computer Security Institute's annual *Computer Crime and Security Survey* is another source of information. In 2007, the survey was based on the responses of almost 500 security practitioners in U.S. corporations, government agencies, financial

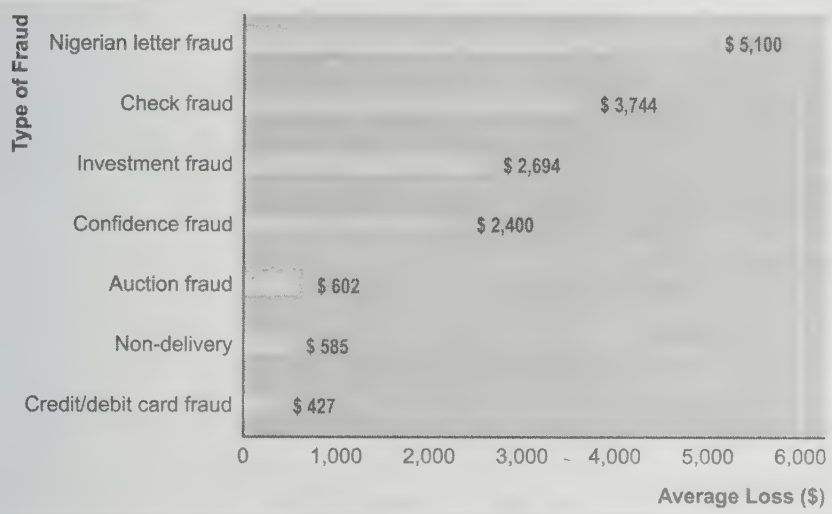
CATEGORIES OF INTERNET CRIME COMPLAINTS REPORTED TO THE IC3



This figure illustrates the top 5 categories of reported complaints to the FBI's Internet Crime Complaint Center. The most common complaint involves auction fraud, accounting for about 45% of reported complaints, followed by non-delivery of merchandise or payment.

SOURCE: Based on data from National White Collar Crime Center and the Federal Bureau of Investigation, 2007.

AVERAGE REPORTED LOSSES FOR VARIOUS TYPES OF INTERNET COMPLAINTS



The average loss for the top seven categories of Internet complaints ranges from a high of $5,100 for Nigerian letter fraud to around $430 for credit/debit card fraud.

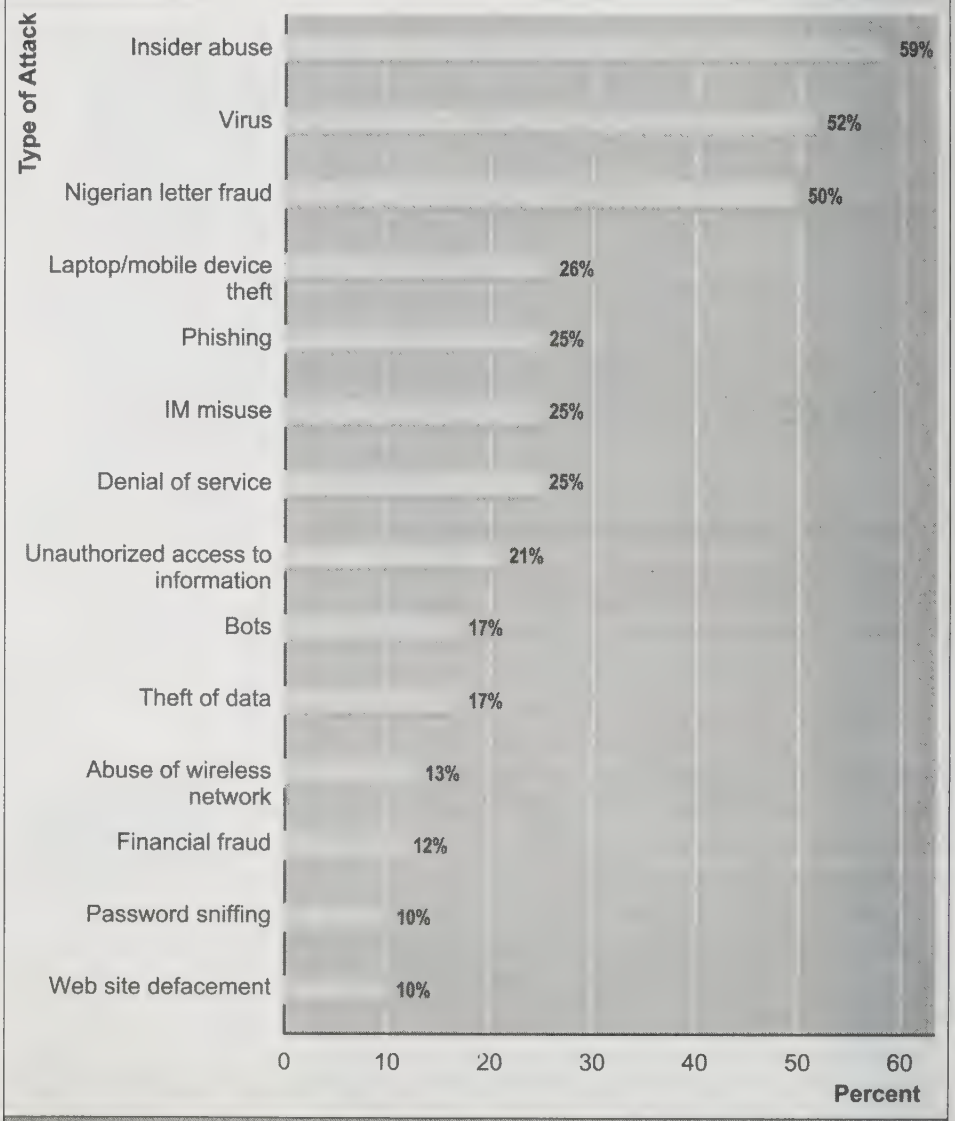
SOURCE: Based on data from National White Collar Crime Center and the Federal Bureau of Investigation, 2007.

institutions, medical institutions, and universities. The survey reported that 46% of responding organizations experienced a computer security incident within the past year. **Figure 5.3** illustrates the various types of attacks against computer systems reported. Not all of these necessarily involve e-commerce, although many of them do. The total loss reported was $67 million, and the average annual loss was approximately $350,000. The most costly categories of attacks were financial fraud ($21 million), viruses ($8 million), and system penetration by an outsider ($6.8 million) (Computer Security Institute, 2007).

Reports issued by security product providers, such as Symantec, are another source of data. Symantec, for instance, issues a semi-annual *Internet Security Threat Report*, based on 40,000 sensors monitoring Internet activity in over 180 countries, and malicious code reports from over 120 million systems that utilize Symantec's anti-virus products. In the first half of 2007, over 200,000 new malicious code threats were reported to Symantec, a 185% increase over the second half of 2006. It observed an average of about 52,000 active bot-infected computers per day and detected a total of 196,860 unique phishing messages, an 18% increase over the last six months of 2006 (Symantec, 2007a). However, Symantec does not attempt to quantify any actual crimes and/or losses related to these threats.

Online credit card fraud and phishing attacks are perhaps the most high-profile form of e-commerce crimes. Although the average amount of credit card fraud loss experienced by any one individual is typically relatively small (for instance, about

FIGURE 5-3 TYPES OF ATTACKS AGAINST COMPUTER SYSTEMS (CYBERCRIME)



The most common attacks against computer systems are insider abuse of Internet access, viruses, laptop and mobile device theft, phishing, IM misuse, and denial of service. Some of these are specifically related to e-commerce, while others are not.

SOURCE: Based on data from Computer Security Institute, 2007.

$430 for those credit card/debit card fraud complaints reported in 2006 to the Internet Crime Complaint Center), the overall amount is substantial. The research firm CyberSource estimates online credit card fraud in the United States amounted to about $3 billion in 2006 (CyberSource, 2007). The overall rate of online credit card

fraud is estimated to be about 1.6%–1.8% of all online card transactions, roughly twice the rate of offline credit card fraud. As a percentage of all e-commerce revenues, credit card fraud is declining as merchants and credit companies expand security systems to prevent the most common types of low-level fraud. But 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 "identify theft," described further later in this chapter, as a major online/offline type of fraud, may well increase markedly the incidence and amount of credit card fraud. Around 15 million Americans experienced identity theft in 2006 and lost an average of $3,257 (eMarketer, Inc., 2007). Many of these losses involved 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 so-called "underground economy servers." There are several thousand known underground economy servers around the world that sell stolen information (about half of these are in the United States). **Table 5.1** lists some recently observed prices.

Finding these servers is difficult for the average user (and for law enforcement agencies), and you need to be vetted by other criminals before gaining access. This vetting process takes place through e-mail exchanges of information, money and reputation. Criminals have fairly good, personalized security!

Note that not every cybercriminal is necessarily after money. In some cases, such criminals aim to just deface, vandalize and/or disrupt a Web site, rather than actually steal goods or services. The cost of such an attack includes not only the time and effort to make repairs to the site but also damage done to the site's reputation and image as well as revenues lost as a result of the attack.

TABLE 5.1 THE UNDERGROUND ECONOMY MARKETPLACE

U.S. credit card	$.50–$5
A full identity (U.S. bank account, credit card, date of birth, social security, etc.)	$10–$150
Bank account	$30–$400
A single compromised computer	$6–$20
Social security number	$5–$7
Phishing Web site hosting	$3–$5
Skype account	$12
World of Warcraft account-one month	$10

SOURCE: Based on data from Symantec, 2007a, 2007b.

So, what can we can conclude about the overall size of cybercrime? Cybercrime against e-commerce sites is dynamic and changing all the time, with new risks appearing often. The amount of losses to businesses appears to be significant but stable, and may represent a declining percentage of overall sales, because firms have invested in security measures to protect against the simplest crimes. Individuals face new risks of fraud, many of which (unlike credit cards where federal law limits the loss to $50 for individuals) involve substantial uninsured losses involving debit cards and bank accounts. 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? Any time 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. In fact, you might pay and get nothing! Worse, someone steals your money while you are at the market! As a merchant in the market, your risk is that you don't get paid for what you sell. Thieves take merchandise and then either walk off without paying anything, or pay you with a fraudulent instrument, stolen credit card, or forged currency.

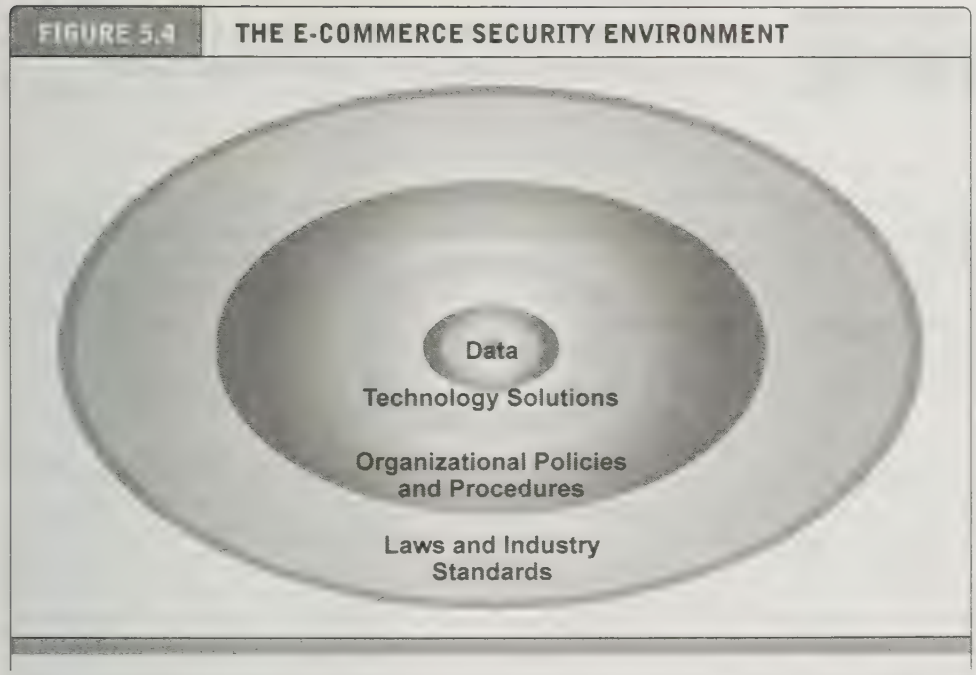
E-commerce merchants and consumers face many of the same risks as participants in traditional commerce, albeit in a new digital environment. Theft is theft, regardless of whether it is digital theft or traditional theft. Burglary, breaking and entering, embezzlement, trespass, malicious destruction, vandalism—all crimes in a traditional commercial environment—are also present in e-commerce. However, reducing risks in e-commerce is a complex process that involves new technologies, organizational policies and procedures, and new laws and industry standards that empower law enforcement officials to investigate and prosecute offenders. **Figure 5.4** illustrates the multi-layered nature of e-commerce security.

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

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 forever is not needed, 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, days, or years. 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.

FIGURE 5.4 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.

DIMENSIONS OF E-COMMERCE SECURITY

There are six key dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability (see **Table 5.2**).

Integrity refers to the ability to ensure that information being displayed on a Web site, 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.

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

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.

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

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 Web site 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.

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

TABLE 5.2 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive 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?

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

privacy
the ability to control the use of information about oneself

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

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 not only violates the confidentiality of the data, but also the privacy of the individuals who supplied the information.

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

E-commerce security is designed to protect these six dimensions. When any one of them is compromised, it is a security issue.

THE TENSION BETWEEN SECURITY AND OTHER VALUES

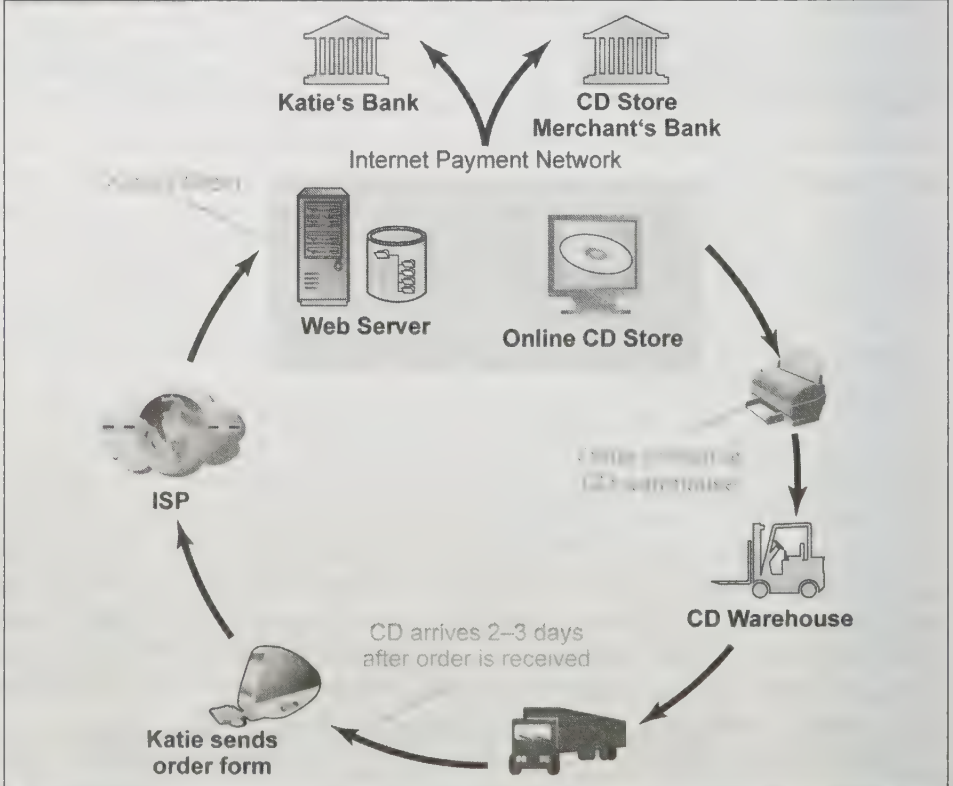
Can there be too much security? The answer is yes. Contrary to what some may believe, security is not an unmitigated good. Computer security adds overhead and expense to business operations, and also gives criminals new opportunities to hide their intentions and their crimes.

and explosive construction, tactical coordination of imminent attacks, and building a larger terrorist community of like-minded people. The Internet is both anonymous and pervasive, an ideal communication tool for criminal and terrorist groups.

5.2 SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT

From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the client, the server, and the communications pipeline. **Figure 5.5** illustrates a typical e-commerce transaction with a consumer using a credit card to purchase a product. **Figure 5.6** 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.

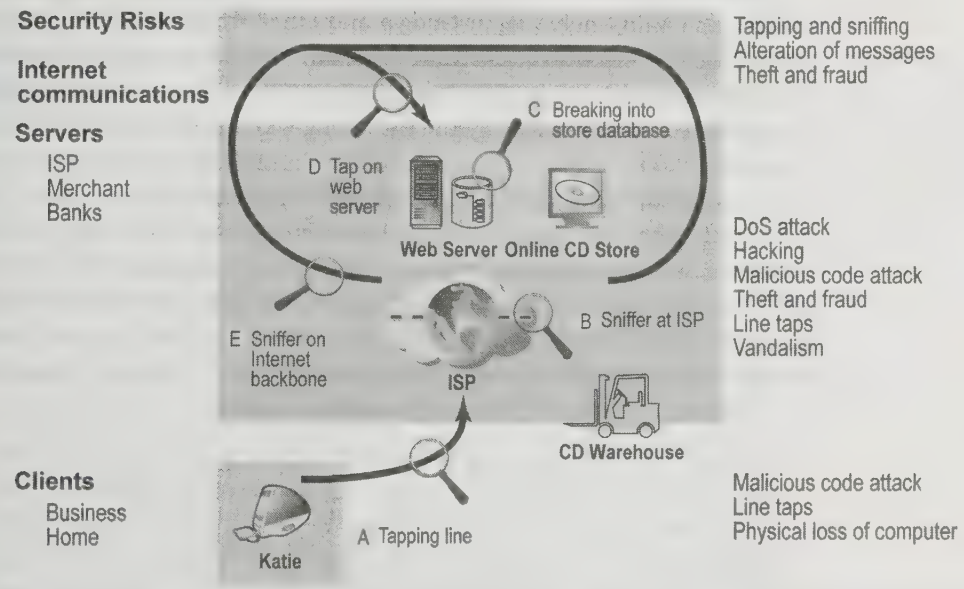
FIGURE 5.5 A TYPICAL E-COMMERCE TRANSACTION



In a typical e-commerce transaction, the customer uses a credit card and the existing credit payment system. The transaction has many vulnerable points.

SOURCE: Boncella, 2000.

FIGURE 5.6 VULNERABLE POINTS IN AN E-COMMERCE TRANSACTION



There are three vulnerable points in e-commerce transactions: Internet communications, servers, and clients.
SOURCE: Boncella, 2000.

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, unwanted programs, phishing and identity theft, hacking and cybervandalism, credit card fraud/theft, spoofing (pharming) and spam (junk) Web sites, Denial of Service (DoS) and Distributed Denial of service (DDoS) attacks, sniffing, insider attacks, and finally, poorly designed server and client software.

MALICIOUS CODE

Malicious code (sometimes referred to as "malware") includes a variety of threats such as viruses, worms, Trojan horses, and bots. A Microsoft test of its malicious software removal tool found that 62% of 5.7 million home and business PCs had active malware installed (Bloor, 2007). Malicious code in the past often was intended simply to impair computers, and was often authored by a lone hacker, but increasingly the intent is to steal e-mail addresses, logon credentials, personal data and financial information. Increasingly, malicious code is used to develop integrated malware networks that organize the theft of information and money.

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

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

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

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.

One of the latest innovations in virus distribution is to embed them in the online advertising chain, including at Google and other ad networks. For instance, in May 2007, Google users who clicked on Tomshardware.com were re-directed to a server that downloaded viruses and destroyed computers. Approximately 100,000 computers were affected. A recent survey of search engine text ads found that 7% led to suspicious sites (Steel, 2007). Viruses embedded in PDF files have also been discovered. Virus authors are also increasingly using links embedded within e-mail instead of the more traditional file attachments to infect computers. The links lead directly to a malicious code download or Web sites that include malicious JavaScript code (Keizer, 2007). 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.

Computer viruses fall into several major categories as follows:

- *Macro viruses* are application-specific, meaning that the virus affects only the application for which it was written, such as Microsoft Word, Excel, or PowerPoint. When a user opens an infected document in the appropriate application, the virus copies itself to the templates in the application, so that when new documents are created, they are infected with the macro virus as well. Macro viruses can easily be spread when sent in an e-mail attachment.
- *File-infecting viruses* usually infect executable files, such as *.com, *.exe, *.drv, and * .dll files. They may activate every time the infected file is executed by copying themselves into other executable files. File-infecting viruses are also easily spread through e-mails and any file transfer system.
- *Script viruses* are written in script programming languages such as VBScript (Visual Basic Script) and JavaScript. The viruses are activated simply by double-clicking an infected *.vbs or *.js file. The ILOVEYOU virus (also known as the Love Bug), which overwrites *.jpg and *.mp3 files, is one of the most famous examples of a script virus.

Viruses are often combined with a worm. Indeed, most researchers agree that classic viruses—the original malicious programs—have become much less common, while the far more dangerous worm has grown exponentially. Some of the reason is simple: viruses infect a single computer, and may destroy but produce very little cash. As the nature of the criminal changes from amateur hacker to professional criminal interested in cash, it is much more lucrative to create a worm that can propagate from one computer to another, perhaps to millions.

worm
malware that is designed to spread from computer to computer

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. For example, the Slammer worm, which targeted a known vulnerability in Microsoft's SQL Server database software, 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. Other well-known worms include the MyDoom worm, the Sasser worm, the Zotob worm, and the Nymex worm (Symantec, 2007; United States Government Accountability Office, 2005).

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. According to Symantec, of the top 10 new malicious code families detected in the first six months of 2007, four were Trojans; during the first half of 2007, Trojans made up 54% of the volume of the top 50 malicious code reports, an increase over the 45% reported in the final six months of 2006; and when measured by potential infections, Trojans accounted for 73% of the top 50 malicious code samples, up from 60% in the previous period (Symantec, 2007). In August 2007, Monster.com suffered a highly publicized attack from a Trojan horse called Infostealer.Monstres that stole more than 1.6 million records, such as names, e-mail addresses, home addresses, and phone numbers of job seekers who had filed resumes with Monster (Kreizer, 2007b).

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

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, and 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 Distributed Denial of Service attack (described later), stealing information from computers, and storing network traffic for later analysis. In the first six months of 2007, Symantec identified an average of 52,771 active bot-infected computers per day and observed over 5 million distinct bot-infected computers. Arguably, bots and bot networks are the single most important threat to the Internet and e-commerce in 2007 because they can be used to launch very large-scale attacks using many different techniques. In 2007, the authors of the Storm worm (which can also be described as a Trojan horse) assembled a massive botnet to propagate the worm. It is estimated that 5,000 to 6,000 computers are dedicated to spreading the worm through the use of e-mail with infected attachments, with over 1.2 billion virus messages sent by the botnet since January 2007 (Gaudin, 2007).

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

botnet
collection of captured bot computers

Malicious code is a threat at both the client and the server level, although servers generally engage in much more thorough anti-virus activities than do consumers. At the server level, malicious code can bring down an entire Web site, 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 5.3** lists some well-known examples of malicious code.

TABLE 5-3 NOTABLE EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Netsky.P	Worm/Trojan horse	First appeared in early 2003 and was still one of the most common computer worms in 2007. It spreads by gathering target e-mail addresses from the computers it infects, and sending e-mail to all recipients from the infected computer. It is commonly used by bot networks to launch spam and Denial of Service attacks.
Storm (Peacomm, NuWar)	Worm/Trojan horse	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.
Stration	Worm	Most common new worm in 2007. Installs other scripts and bots.
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.
Sasser	Worm	First appeared in 2004. Exploited a vulnerability in LSASS, causing network problems.
Mydoom	Worm	First appeared in January 2004. One of the fastest-spreading mass-mailer worms. Still in the top 10 in August 2007.
Slammer	Worm	Launched in January 2003. Caused widespread problems.
Klez	Worm	Most prolific virus of 2002. Klez is distributed via an e-mail with a random subject line and message body. Once launched, the worm sends itself to all addresses in the Windows Address Book, the database of instant-messaging program ICQ, and local files. Klez also attempts to disable anti-virus software and drops another virus in the user's system that tries to infect executable files there and across network filing systems.
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, Melissa was 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.

While the number of viruses and worms is increasing, so too has prosecution of those who create viruses. Increasingly, European and Asian authorities are coordinating arrests with American authorities. In the United States, the FBI's Operation BotRoast has resulted in a number of arrests (FBI, 2007). In 2006, a Moroccan teenager was sent to jail for two years for releasing the Zotob worm virus that ravaged U.S. computer networks. In July 2005, the 18-year-old creator of the Sasser worm was convicted in Germany on charges including computer sabotage.

UNWANTED PROGRAMS

In addition to malicious code, the e-commerce security environment is further challenged by unwanted programs such as adware, browser parasites, spyware, and other applications that install themselves on a computer, typically without the user's informed consent. Such programs are increasingly being found on social networking and user-generated content sites where users are fooled into downloading them (Symantec, 2007). Once installed, these applications are usually exceedingly difficult to remove from the computer.

Adware (described further in Chapter 7) 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. ZangoSearch and PurityScan are examples of adware programs that open the Web pages or display pop-up ads of partner sites when certain keywords are used in Internet searches. 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. For example, Websearch is an adware component that modifies Internet Explorer's default home page and search settings.

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

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). One example of spyware is SpySheriff, which claims to be a spyware removal program but is actually a malicious spyware application. Spyware (along with phishing, described in the next section) is often used for identity theft.

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

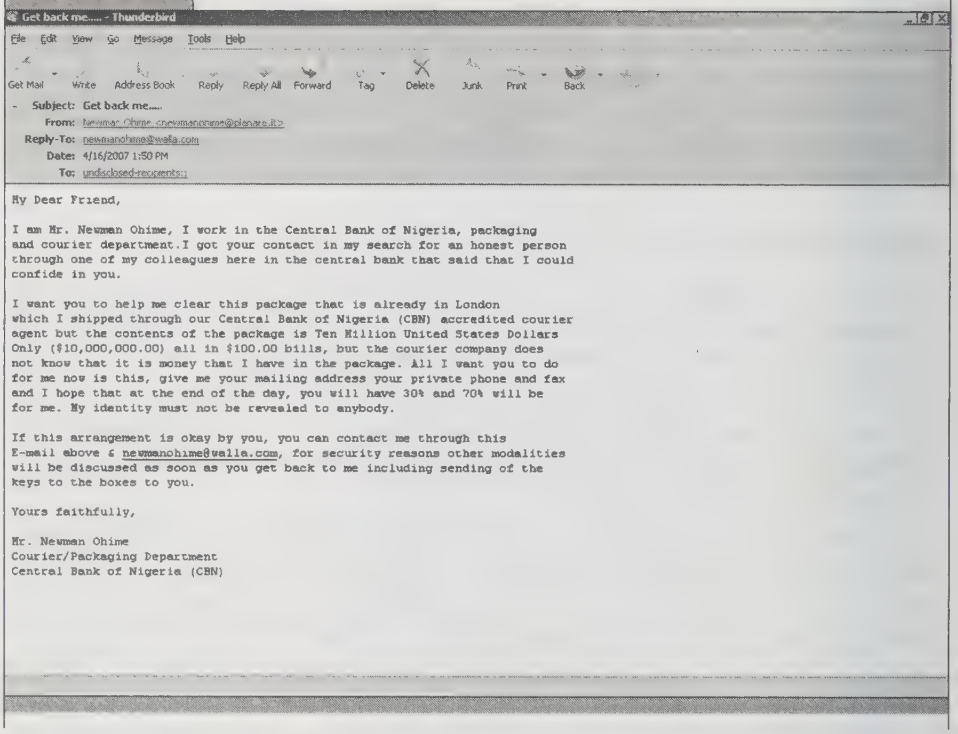
PHISHING AND IDENTITY THEFT

Phishing is any deceptive, online attempt by a third party to obtain confidential information for financial gain. Phishing attacks do not involve malicious code but instead rely on straightforward misrepresentation and fraud, so-called "social engineering" techniques. The most popular phishing attack 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 a million dollars. This type of e-mail scam is popularly known as a "Nigerian letter" scam (see **Figure 5.7**).

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

Thousands of other phishing attacks use other scams, some pretending to be eBay, PayPal, or Citibank writing to you for "account verification." Click on a link in

FIGURE 5.7 AN EXAMPLE OF A NIGERIAN LETTER E-MAIL SCAM

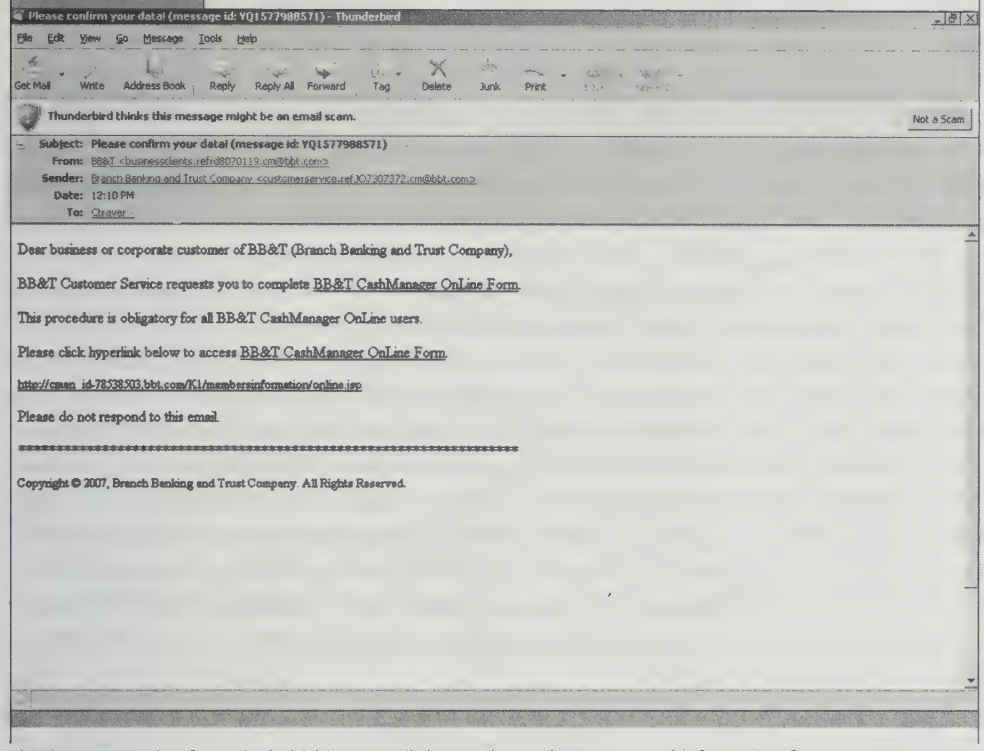


This is an example of a typical Nigerian letter e-mail scam.

the e-mail and you will be taken to a Web site controlled by the scammer, and prompted to enter confidential information about your accounts, such as your account number and PIN codes (see **Figure 5.8**). 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 ("spoof") a Web site that purports to be a legitimate financial institution and con users into entering financial information. 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 theft). Phishing attacks are one of the fastest-growing forms of e-commerce crime. During the first six months of 2007, Symantec detected 197,000 unique new phishing e-mail messages, an increase of 18% compared to the second half of 2006 (Symantec, 2007). In October 2007, OpenDNS published the PhishTank Annual Report, based on over 300,000 phishing scams it examined. The report found that the top two spoofed brands were eBay and PayPal, with a variety of banks, the IRS, and several large retailers (Amazon and Wal-Mart) rounding out the top 10. It also found that just over 30% of phishing Web

FIGURE 5.8 AN EXAMPLE OF A PHISHING ATTACK



This is an example of a typical phishing e-mail that seeks to obtain personal information from an unwary respondent.

sites were hosted on U.S.-based networks, but that the three IP addresses with the most attacks—responsible for a total of 18% of all verified phishing Web sites—were located in Korea, Turkey, and Chile (OpenDNS, 2007).

Many of the security vulnerabilities described throughout this section use what are called "social engineering" techniques to propagate. These techniques involve fraud or misrepresentation, or in other words, pretending to be something that it is not. For instance, the Netsky.P worm uses an e-mail message that takes the form of an e-mail delivery notification to trick recipients into thinking that the e-mail is from a valid source, encouraging them to open an attached file that, in reality, is an executable program that contains a virus or worm. Once the attachment is opened, the worm begins to execute on the computer. Social engineering not only aids the worm in getting the target recipient to open the infected e-mail, it also allows the worm to evade content filters or scanners, often by masquerading as a compressed zip file.

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

HACKING AND CYBERVANDALISM

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 Web sites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use. Hackers and crackers typically are computer aficionados excited by the challenge of breaking into corporate and government Web sites. Sometimes they are satisfied merely by breaking into the files of an e-commerce site. Others have more malicious intentions and commit **cybervandalism**, intentionally disrupting, defacing, or even destroying the site.

cybervandalism
intentionally disrupting, defacing, or even destroying a site

For instance, Robert Lyttle of San Francisco and Benjamin Stark of St. Petersburg, Florida, were convicted of breaking into and "hacking" a computer at NASA's Ames Research Center in Moffett Field, California. They stole information about members of the agency's Astrobiology Institute and used that information to deface the home page of the NASA Astrobiology Institute. Calling themselves "The Deceptive Duo," Lyttle and Stark stated that their attacks were intended to demonstrate vulnerabilities in the government's computer security systems. The pair also hacked into the Defense Department's Defense Logistics Information Service Web site and the agency's Office of Health Affairs. Lyttle pleaded guilty to the attacks, and the U.S. District Court in Oakland, California, sentenced him to four months in prison, restitution payment of $71,181, and three years probation. Stark, who also pleaded guilty, was sentenced to two years probation and to pay $29,006 in restitution (Butterfield, 2005).

The hacker phenomenon has diversified over time. In general, benign hacking and defacement hacking has receded as law enforcement and private agencies learn how to detect perpetrators. Hacker activities have broadened beyond mere system intrusion to include theft of goods and information, as well as vandalism and system damage. Financial hacking is on the rise, especially from foreign countries. For instance, hackers invaded the Web sites of the Miami Dolphins in January 2007, and the World Cup Web site, in order to install key-logging software on visitors' computers.

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 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 clients that they will not be prosecuted for their efforts to break in.

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

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

black hats
hackers who act with the intention of causing harm

Somewhere in the middle are the **grey hats**, hackers who believe they are pursuing some greater good by breaking in and revealing system flaws. Grey hats discover weaknesses in a system's security, and then publish the weakness without disrupting the site or attempting to profit from their finds. Their only reward is the

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

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.

CREDIT CARD FRAUD/THEFT

Theft of credit card data is one of the most feared occurrences on the Internet. Fear that credit card information will be stolen frequently prevents users from making online purchases. Interestingly, this fear appears to be largely unfounded. Incidences of stolen credit card information are much lower than users think, around 1.6%–1.8% of all online card transactions (CyberSource Corporation, 2007).

In traditional commerce, there is substantial credit card fraud, but the consumer is largely insured against losses by federal law. In the past, the most common cause of credit card fraud was 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). Federal law limits the liability of individuals to $50 for a stolen credit card. For amounts over $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.

But 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 are stored. The largest and most damaging mass credit card theft to date occurred at TJX Companies, owner of 2,500 retail stores. Information from 47.5 million credit and debit cards was stolen by hackers who gained access to TJX's customer information database via a poorly protected wireless local area network in 2003. The theft was not discovered until 2006, and was not reported until 2007. The information was sold on underground economy sites to criminals who subsequently made hundreds of thousands of purchases, both offline and online (Dash, 2007; Vijayan, 2007).

International orders have been particularly prone to repudiation. 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.

The solution for many Web sites is to institute new identity verification mechanisms that are currently in development; these will be discussed in the next section. Until a customer's identity can be guaranteed, online companies are at a much 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. Except for large businesses conducting transactions over the Internet, the law has had little impact on B2C commerce, but that may be changing.

SPOOFING (PHARMING) AND SPAM (JUNK) WEB SITES

spoof
to misrepresent oneself by using fake e-mail addresses or masquerading as someone else

Hackers attempting to hide their true identity often **spoof**, or misrepresent themselves by using fake e-mail addresses or masquerading as someone else. Spoofing a Web site is also called "pharming," which involves 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. Spam Web sites are a little different. These are sites that promise to offer some product or service, but in fact are 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 Web sites.

Although spoofing does not directly damage files or network servers, it threatens the integrity of a site. For example, if hackers redirect customers to a fake Web site 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 products ordered—and then send them on to the true site for processing and delivery. Customers become dissatisfied with the improper order shipment and the company may have huge inventory fluctuations that impact its operations.

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

Junk or spam Web sites 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, post their names on open Web forums, and redirect traffic to known spammer-redirection domains such as vip-online-search.info, searchadv.com, and webresourses.info. Recent research on junk Web sites found more than 30% of the results on keywords "drugs" and "ringtones" led to fake Web pages supported by major advertisers. One study found that 11% of the pages returned for 1,000 keywords were fake (Wang, et al., 2007).

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

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

In a **Denial of Service (DoS)** attack, hackers flood a Web site with useless 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. According to Symantec, during the first half of 2007, the United States was subject to the most DoS attacks, accounting for 61% of the worldwide total (Symantec, 2007). DoS attacks typically cause a Web site 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 removing the DoS attack.

A **Distributed Denial of Service (DDoS)** attack uses numerous 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 Web sites such as Yahoo and Microsoft have experienced such attacks, making the companies aware of their vulnerability and the need to introduce new measures to prevent future attacks. The largest DDoS attack to date occurred in February 2007, when a botnet composed of several thousand computers attempted to bring down the part of the Internet domain name system operated by VeriSign. The attack affected all of the thirteen domain name servers operated by VeriSign, including the .com and .org domains (Markoff, 2007). The attack impeded but did not bring down any of the servers. Had it succeeded, the Internet itself would have failed for a period of time.

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

SNIFFING

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 e-mail messages, company files, and confidential reports. The threat of sniffing is that confidential or personal information will be made public. For both companies and individuals, such an occurrence can be disruptive.

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

E-mail wiretaps are a variation on the sniffing threat. An e-mail wiretap is hidden code in an e-mail message that allows someone to monitor all succeeding messages forwarded with the original message. E-mail wiretaps can be installed on servers and client computers. For instance, 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 (Associated Press, 2005). Congress adopted a new amendment to the 1978 Foreign Intelligence Surveillance Act, known as FISA, that provides 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).

INSIDER ATTACKS

We tend to think of security threats to a business as originating outside the organization. In fact, the largest financial threats to business institutions come not from robberies but from embezzlement by insiders. Bank employees steal far

more money than bank robbers. The same is true for e-commerce sites. Some of the largest disruptions to service, destruction to sites, and diversion of customer credit data and personal information have come from insiders—once trusted employees. Employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace. The 2007 CSI survey reports that insider abuse of systems was the second most frequent type of attack during the preceding 12 months, and that 64% of survey respondents believed that insiders contributed to some portion of the firm's financial losses during the previous year (Computer Security Institute, 2007). A Michigan State University study found that as much as 70% of all identity theft, including credit card theft, is the work of "insiders" (Borden, 2007). In some instances, the insider might not have criminal intent, but inadvertently expose data that can then be exploited by others. For instance, in September 2007, Citigroup confirmed that it was investigating a data breach that involved the names, social security numbers, and credit card information of over 5,000 customers by an employee of its ABN Amro Mortgage Group unit onto the LimeWire P2P file-sharing network (Vass, 2007).

POORLY DESIGNED SERVER AND CLIENT SOFTWARE

Many security threats prey on poorly designed server and client 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. Each year security firms identify about 5,000 software vulnerabilities in Internet and PC software. For instance, in 2007, Symantec identified 39 vulnerabilities in Internet Explorer, 34 in Mozilla browsers, 25 in Apple Safari, and 7 in Opera. Some of these vulnerabilities were critical (Symantec, 2007). All the top 10 Internet attacks launched in 2007 were attacks against the Microsoft Windows server and client software, exploiting weaknesses in Microsoft's Win32 application programming interface (API). 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. The port typically attacked is TCP port 445. However, given their complexity and design objectives, all operating systems and application software, including Linux and Macintosh, have vulnerabilities. There are also a growing number of "zero-day" vulnerabilities, where the vulnerability is unknown to security experts and is actively exploited before there is a patch available, requiring firms to scurry to develop patches. In the single week of August 13, 2007, the U.S. Computer Emergency Readiness Team (US-CERT; Department of Homeland Security) reported on 98 newly discovered vulnerabilities in server and application software, 28 of them rated "high severity" (US-CERT, 2007).

5.3 TECHNOLOGY SOLUTIONS

At first glance it might seem like there is not much that can be done about the onslaught of security breaches on the Internet. Reviewing the security threats in the previous section, it is clear that the threats to e-commerce are very real, potentially devastating, and likely to be increasing in intensity along with the growth in e-commerce. 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 5.9** illustrates the major tools available to achieve site security. In the next section, we describe these tools in greater detail.

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

FIGURE 5.9 TOOLS AVAILABLE TO ACHIEVE SITE SECURITY

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

communications. This is very different from a private network where a dedicated communication line is established between two parties. A number of tools are available to protect the security of Internet communications, the most basic of which is message encryption.

ENCRYPTION

encryption
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 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 5.2:

- *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.

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

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."

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 Encryption

In order to decipher these messages, the receiver would have to know the secret cipher that was used to encrypt the plain text. This is called **symmetric key encryption** or **secret key encryption**. In symmetric key encryption, 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 encryption was used extensively throughout World War II and is still a part of Internet encryption.

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

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 encryption requires that both parties share the same key. In order to

everyone using computers and networks like the Internet has a role to play. The Guidelines represent the consensus views of all 30 OECD member countries and support the OECD's larger goal of promoting economic growth, trade, and development.

5.3 PAYMENT SYSTEMS

TYPES OF PAYMENT SYSTEMS

In order to understand e-commerce payment systems, you first need to be familiar with the various types of generic payment systems. Then you will be able to clarify the different requirements that e-commerce payments systems must meet and identify the opportunities provided by e-commerce technology for developing new types of payment systems. There are five main types of payment systems: cash, checking transfer, credit cards, stored value, and accumulating balance.

Cash

cash
legal tender defined by a national authority to represent value

Cash, which is legal tender defined by a national authority to represent value, is the most common form of payment in terms of number of transactions. The key feature of cash is that it is instantly convertible into other forms of value without the intermediation of any other institution. For instance, free airline miles are not cash because they are not instantly convertible into other forms of value—they require intermediation by a third party (the airline) in order to be exchanged for value (an airline ticket). Private organizations sometimes create a form of private cash called *scrip* that can be instantly redeemed by participating organizations for goods or cash. Examples include trading stamps, "point" programs, and other forms of consumer loyalty currency.

Why is cash still so popular today? Cash is portable, requires no authentication, and provides instant purchasing power for those who possess it. Cash allows for micropayments (payments of small amounts). The use of cash is "free" in that neither merchants nor consumers pay a transaction fee for using it. Using cash does not require any complementary assets, such as special hardware or the existence of an account, and it puts very low cognitive demands on the user. Cash is anonymous and difficult to trace, and in that sense it is "private." Other forms of payment require significant use of third parties and leave an extensive digital or paper trail.

float
the period of time between a purchase and actual payment for the purchase

On the other hand, cash is limited to smaller transactions (you can't easily buy a car or house with cash), it is easily stolen, and it does not provide any "**float**" (the period of time between a purchase and actual payment for the purchase); when it is spent, it is gone. With cash, purchases tend to be final and irreversible (i.e., they are irrefutable) unless otherwise agreed by the seller.

Checking Transfer

checking transfer
funds transferred directly via a signed draft or check from a consumer's checking account to a merchant or other individual

A **checking transfer**, which represents funds transferred directly via a signed draft or check from a consumer's checking account to a merchant or other individual, is the second most common form of payment in the United States in terms of number of transactions, and the most common in terms of total amount spent.

Checks can be used for both small and large transactions, although typically they are not used for micropayments (less than $1). Checks have some float (it can take up to 10 days for out-of-state checks to clear), and the unspent balances can earn interest. Checks are not anonymous and require third-party institutions to work. Checks also introduce security risks for merchants: They can be forged more easily than cash, so authentication is required. For merchants, checks also present some additional risk compared to cash because they can be canceled before they clear the account or they may bounce if there is not enough money in the account.

Credit Card

A **credit card** represents an account that extends credit to consumers, permits consumers to purchase items while deferring payment, and allows consumers to make payments to multiple vendors at one time. **Credit card associations** such as Visa and MasterCard are nonprofit associations that set standards for the **issuing banks**—such as Citibank—that actually issue the credit cards and process transactions. Other third parties (called **processing centers** or **clearinghouses**) usually handle verification of accounts and balances. Credit card issuing banks act as financial intermediaries, minimizing the risk to transacting parties.

Credit cards offer consumers a line of credit and the ability to make small and large purchases instantly. They are widely accepted as a form of payment, reduce the risk of theft associated with carrying cash, and increase consumer convenience. Credit cards also offer consumers considerable float. With a credit card, for instance, a consumer typically need not actually pay for goods purchased until receiving a credit card bill 30 days later. Merchants benefit from increased consumer spending resulting from credit card use, but they pay a hefty transaction fee of 3% to 5% of the purchase price to the issuing banks. In addition, federal Regulation Z places the risks of the transaction (such as credit card fraud, repudiation of the transaction, or nonpayment) largely on the merchant and credit card issuing bank. Regulation Z limits cardholder liability to $50 for unauthorized transactions that occur before the card issuer is notified. Once a card is reported stolen, consumers are not liable for any subsequent charges.

Credit cards have less finality than other payment systems because consumers can refute or repudiate purchases under certain circumstances, and they limit risk for consumers while raising risk for merchants and bankers.

credit card
represents an account that extends credit to consumers, permits consumers to purchase items while deferring payment, and allows consumers to make payments to multiple vendors at one time

credit card association
nonprofit association that sets standards for issuing banks

issuing bank
bank that actually issues credit cards and processes transactions

processing center (clearinghouse)
institution that handles verification of accounts and balances

Stored Value

Accounts created by depositing funds into an account and from which funds are paid out or withdrawn as needed are **stored-value payment systems**. Stored-value payment systems are similar in some respects to checking transfers—which also store funds—but do not involve writing a check. Examples include debit cards, gift certificates, prepaid cards, and smart cards (described in greater detail later in the chapter). **Debit cards** immediately debit a checking or other demand-deposit account. For many consumers, the use of a debit card eliminates the need to write a paper check. Today, there are nearly 300 million debit cards in use nationwide, and they are used in more than a quarter of all purchases made in U.S. retail stores. However, because debit cards are

stored-value payment system
account created by depositing funds into an account and from which funds are paid out or withdrawn as needed

debit card
immediately debits a checking or other demand-deposit account

dependent on funds being available in a consumer's bank account, larger purchases are still typically paid for by credit card, and their use in the United States still lags behind that of other developed nations, in part because they do not have the protections provided by Regulation Z and they do not provide any float.

P2P payment systems such as PayPal (discussed further in Section 5.6) are variations on the stored value concept. P2P payment systems do not insist on prepayment, but do require an account with a stored value, either a checking account with funds available or a credit card with an available credit balance. PayPal is often referred to as a P2P payment system because it allows small merchants and individuals to accept payments without using a merchant bank or processor to clear the transaction.

Accumulating Balance

accumulating balance payment system
account that accumulates expenditures and to which consumers makes periodic payments

Accounts that accumulate expenditures and to which consumers make periodic payments are **accumulating balance payment systems**. Traditional examples include utility, phone, and American Express accounts, all of which accumulate balances, usually over a specified period (typically a month), and then are paid in full at the end of the period.

Table 5.6 summarizes how payment systems differ on a variety of dimensions and highlights a number of points about payment systems. First, evaluating payment systems is a complex process; there are many dimensions that must be considered. Table 5.6 suggests how difficult it is for entrepreneurs to devise new payment mechanisms to displace current payment systems (cash, checks, and credit cards). As we will discuss below, consumers in the United States have not, as a general matter, accepted alternative online payment systems and rely primarily on credit cards for online payments.

Table 5.6 also suggests that the various parties that have an interest in payment systems (stakeholders) may have different preferences with respect to the different dimensions. The main stakeholders in payment systems are consumers, merchants, financial intermediaries, and government regulators.

Consumers are interested primarily in low-risk, low-cost, refutable (able to be repudiated or denied), convenient, and reliable payment mechanisms. Consumers have demonstrated they will not use new payment mechanisms unless they are equally or more beneficial to them than existing systems. In general, most consumers use cash, checks, and/or credit cards. The specific payment system chosen will change depending on the transaction situation. For instance, cash may be preferred to keep certain transactions private and anonymous, but the same consumer may want a record of transaction for the purchase of a car.

Merchants are interested primarily in low-risk, low-cost, irrefutable (i.e., final), secure, and reliable payment mechanisms. Merchants currently carry much of the risk of checking and credit card fraud, refutability of charges, and much of the hardware cost of verifying payments. Merchants typically prefer payments made by cash, check, and to a lesser extent credit cards, which usually carry high fees and allow transactions to be repudiated after the fact by consumers.

Financial intermediaries, such as banks and credit card networks, are primarily interested in secure payment systems that transfer risks and costs to consumers and

merchants, while maximizing transaction fees payable to themselves. The preferred payment mechanisms for financial intermediaries are checking transfers, debit cards, and credit cards.

Government regulators are interested in maintaining trust in the financial system. Regulators seek to protect against fraud and abuse in the use of payment systems; ensure that the interests of consumers and merchants are balanced against the interests of the financial intermediaries whom they regulate; and enforce information reporting laws. The most important regulations of payment systems in the United States are Regulation Z, Regulation E, and the Electronic Funds Transfer Act (EFTA) of 1978, regulating ATM machines. Regulation Z limits the risk to consumers when using credit cards. In contrast, EFTA and Regulation E place more risk on consumers when using debit or ATM cards. For instance, if you lose an ATM card or debit card, you are potentially liable for any losses to the account. However, in reality, Visa and MasterCard have issued policies that limit consumer risk for loss of debit cards to the same $50 that applies to credit cards.

TABLE 5.6 DIMENSIONS OF PAYMENT SYSTEMS

DIMENSION	CASH	PERSONAL CHECK	CREDIT CARD	STORED VALUE (DEBIT CARD)	ACCUMULATING BALANCE
Instantly convertible without intermediation	yes	no	no	no	no
Low transaction cost for small transactions	yes	no	no	no	yes
Low transaction cost for large transactions	no	yes	yes	yes	yes
Low fixed costs for merchant	yes	yes	no	no	no
Refutable (able to be repudiated)	no	yes	yes	no (usually)	yes
Financial risk for consumer	yes	no	up to $50	limited	no
Financial risk for merchant	no	yes	yes	no	yes
Anonymous for consumer	yes	no	no	no	no
Anonymous for merchant	yes	no	no	no	no
Immediately respendable	yes	no	no	no	no
Security against unauthorized use	no	some	some	some	some
Tamper-resistant	yes	no	yes	yes	yes
Requires authentication	no	yes	yes	yes	yes
Special hardware required	no	no	yes—by merchant	yes—by merchant	yes—by merchant
Buyer keeps float	no	yes	yes	no	yes
Account required	no	yes	yes	yes	yes
Has immediate monetary value	yes	no	no	yes	no

SOURCE: Adapted from MacKie-Mason and White, 1996.

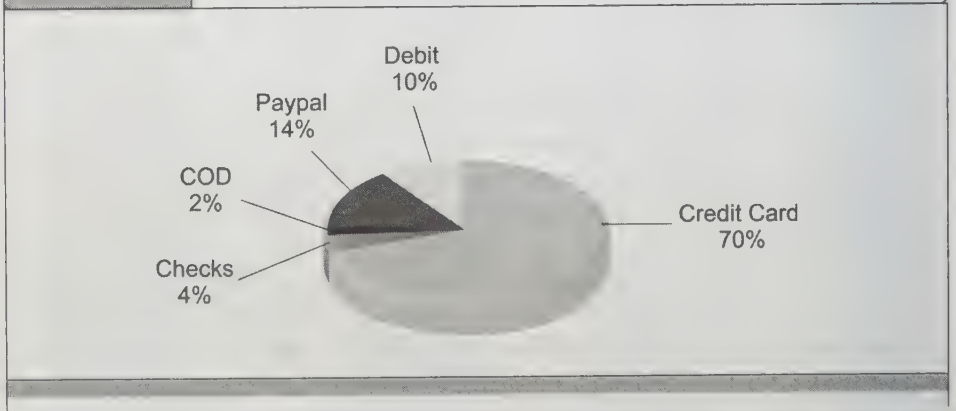
5.6 E-COMMERCE PAYMENT SYSTEMS

The emergence of e-commerce has created new financial needs that in some cases cannot be effectively fulfilled by traditional payment systems. For instance, new types of purchasing relationships—such as auctions between individuals online—have resulted in the need for peer-to-peer payment methods that allow individuals to e-mail payments to other individuals. New types of online information products such as iTunes, video purchases and rentals, newspaper and magazine articles, and other information services require micropayments of less than $5. Yet, for the most part, existing payment mechanisms used in most societies have been able to adapt to the new online environment. E-commerce technology offers a number of possibilities for creating new payment systems that substitute for existing systems, as well as for creating enhancements to existing systems. In this section, we provide an overview of e-commerce payment systems in use today.

In the United States, the primary form of online payment is the existing credit card system. In 2007, credit cards accounted for around 70% of online transactions in the United States. **Figure 5.17** illustrates the approximate usage of various payment types. In general, Americans have been slow to adopt debit cards although their usage is growing and more than 30% of consumers have a debit card. Online, Americans have been far more likely to adopt PayPal than debit cards. PayPal is the most successful online stored value payment system (see the "Online Stored Value Payment Systems" section for more information on PayPal).

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 in the United States. If you plan on operating a Web site in

FIGURE 5.17 ONLINE PAYMENT METHODS IN THE UNITED STATES



Traditional credit cards are the dominant method of payment for online purchases, although PayPal is gaining ground.

SOURCE: Based on data from CyberSource Corporation, 2007; U.S. Census Bureau, 2007; authors' estimates.

Europe, Asia, or Latin America, you will need to develop different payment systems for each region. Consumers in Europe rely for the most part on bank debit cards (especially in Germany) and some credit cards. Online purchases in China are typically paid for by check or cash when the consumer picks up the goods at a local store. In Japan, consumers use postal and bank transfers and CODs, using local convenience stores (konbini) as the pickup and payment point. Japanese consumers also use accumulated balance accounts with the telephone company for Internet purchases made from their home computers.

ONLINE CREDIT CARD TRANSACTIONS

Because credit 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 *MOTO* (Mail Order-Telephone Order) transactions. These types of purchases are also called CNP (Cardholder Not Present) transactions and are the major reason that charges can be disputed later by consumers. Since 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.

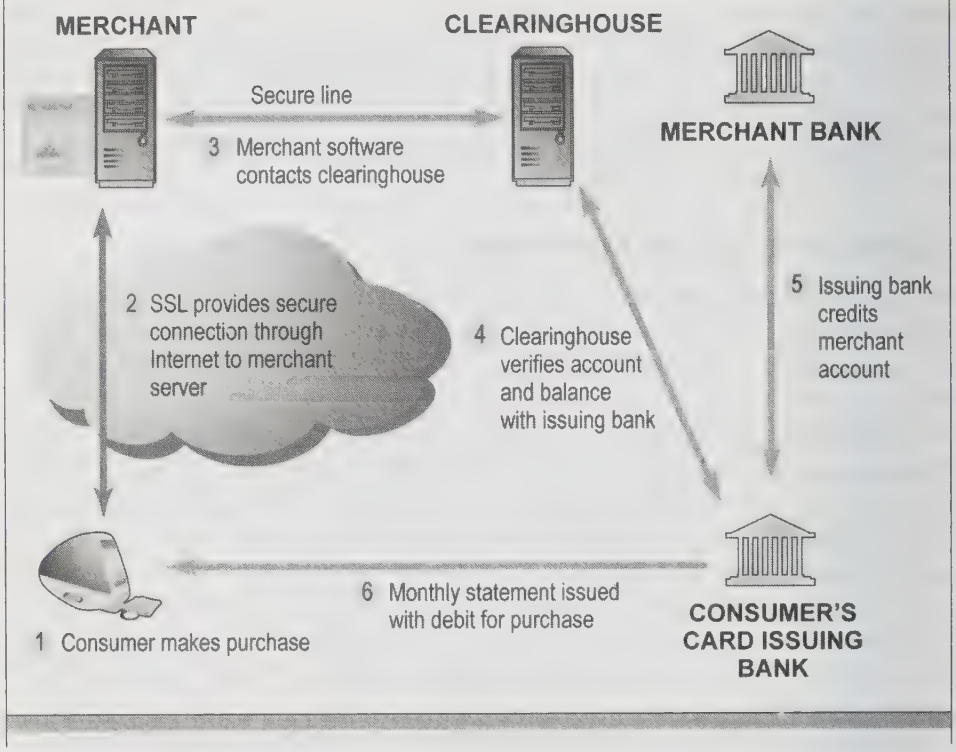
Figure 5.18 illustrates the online credit card purchasing cycle. There are five parties involved in an online credit card purchase: consumer, merchant, clearinghouse, merchant bank (sometimes called the "acquiring bank"), and the consumer's card issuing bank. In order to accept payments by credit card, online merchants must have 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.

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

As shown in Figure 5.18, 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. Using encryption, SSL 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).

FIGURE 5.18 HOW AN ONLINE CREDIT CARD TRANSACTION WORKS



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 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. Authorize.net 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.

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, cost, 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 protocol (SET) in 2000, but this effort failed because it was too complex for consumers and merchants alike.

Credit costs for merchants are also significant—roughly 3.5% of the purchase plus a transaction fee of 20–30 cents per transaction, plus other setup fees. Stored value systems such as PayPal that rely on the credit card system are even more costly: in addition to paying the credit card fee of 3.5%, PayPal tacks on a variable fee of from 1.5%–3% depending on the size of the transaction. The high costs make it undesirable to sell goods that cost less than $10 on the Web. The sale of individual articles, music tracks, or other small items is not particularly feasible with credit cards. One way around this problem is to aggregate a consumer's purchases over a period of time before actually charging the credit card. This is the tack taken by Apple's iTunes Music Store, which charges 99 cents per song. Instead of charging your credit card for each individual song, Apple aggregates any purchases you make within a 24-hour period so that they're posted to your credit card account as a total for the period, not as individual song purchases. iTunes barely breaks even on a 99 cent sale, but can start making money if you purchase several songs. In general, credit companies are opposed to "aggregating" because it reduces their profits.

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.

DIGITAL WALLETS

Aside from credit cards, there are also a number of new forms of payment that have been attempted, with mixed success. These include digital wallets, digital cash, online stored value payment systems, digital accumulating balance systems, and digital checking systems

A **digital wallet** seeks to emulate the functionality of a regular wallet that you carry on your person. The most important functions of a digital wallet are to (a) authenticate the consumer through the use of digital certificates or other encryption methods, (b) store and transfer value, and (c) secure the payment process from the consumer to the merchant. Early efforts by many companies failed to popularize the idea of a digital wallet. Even Microsoft, which offered a proprietary server-side digital wallet with first Passport and then MSN Wallet, ultimately abandoned the effort in February 2005. The latest effort to develop something like a digital wallet is Google's Checkout, which is a payment processing system designed to make online shopping more convenient and easier. It does not store value like PayPal, but communicates a shopper's credit card and personal information necessary for a transaction to the merchant. The merchant receives some additional transaction guarantees that the user has been authenticated by Google. It is not clear at this time how successful this system will be.

digital wallet
emulates the functionality of a regular wallet by authenticating the consumer, storing and transferring value, and securing the payment process from consumer to merchant

DIGITAL CASH

digital cash
an alternative payment system developed for e-commerce in which unique, authenticated tokens representing cash value are tramsmitted from consumers to merchants

Digital cash (sometimes called *e-cash*) was one of the first forms of alternative payment systems developed for e-commerce. The basic idea behind all digital cash systems is payment over the Internet by transmitting unique, authenticated tokens representing cash value from consumer to merchants. In these schemes, users would deposit money in a bank or provide a credit card. Banks would issue digital tokens (unique encrypted numbers) for various denominations of cash, and consumers could "spend" these at merchants' sites. Merchants would in turn deposit these electronic tokens in its bank. DigiCash, First Virtual, and Millicent, all early pioneers in digital cash, no longer offer services in the form originally envisioned. In general, the protocols and practices required to make digital cash a reality were far too complex. However, there are still several firms that are continuing to pursue the idea of digital cash. Some firms, such as E-gold and GoldMoney, have focused on electronic currency backed by gold bullion. E-gold is probably the best known of these firms. Originally established in 1996, E-gold Ltd., a company organized under the laws of the country of Nevis, offers an electronic currency it calls E-gold that is backed by gold bullion.

ONLINE STORED VALUE PAYMENT SYSTEMS

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

Online stored value payment systems permit consumers to make instant, online payments to merchants and other individuals based on value stored in an online account.

PayPal (purchased by eBay in 2002) enables individuals and businesses with e-mail accounts to make and receive payments up to a specified limit. PayPal transferred about $45 billion in payments among individuals and businesses in 2007. PayPal is now available in 190 countries and has about 165 million account holders, of which about 40 million are considered to be active accounts. 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 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. Issues with PayPal include its high cost, and lack of consumer protections when a fraud occurs or a charge is repudiated. PayPal is discussed in further depth in the case study at the end of the chapter.

There are also several different categories of online stored value systems in addition to PayPal. Some, such as Valista, are merchant platforms. Others, such as QPass, are primarily aimed at the micropayments market for wireless carriers and publishers selling individual articles.

smart card
a credit-card sized plastic cards with an embedded chip that stores personal information; can be used to support mobie wireless e-commerce payments

Smart cards are another kind of stored value system based on credit-card-sized plastic cards with embedded chips that store personal information that can be used to support mobile wireless e-commerce payments. They are not used from home PCs to purchase goods, but can be used to pay for generally small ticket items by waving the

card at a reader, or passing it through a reader. Whereas credit cards store a single charge account number in the magnetic strip on the back, smart cards can hold 100 times more data, including multiple credit card numbers and information regarding health insurance, transportation, personal identification, bank accounts, and loyalty programs, such as frequent flyer accounts. This capacity makes them an attractive alternative to carrying a dozen or so credit and ID cards in a physical wallet. Smart cards can also require a password, unlike credit cards, adding another layer of security.

There are actually two types of smart cards—*contact and contactless*—depending on the technology embedded. In order for contact cards to be read, they must be physically placed into a card reader, while contactless cards have an antenna built in that enables transmission of data without direct contact using RFID technology. **Radio frequency identification (RFID)** is a method of automatic identification that uses short range radio signals to identify objects and users. A stored-value smart card, such as a retail gift card purchased in a certain dollar value, is an example of a contact card because it must be swiped through a smart card reader in order for payment to be processed. A highway toll payment system such as EZPass is an example of a contactless smart card because the EZPass device in the card is read by a remote sensor, with the appropriate toll automatically deducted from the card at the end of the trip.

radio frequency identification (RFID)
a method of automatic identification that uses short range radio signals to identify objects and users

Smart cards as payment vehicles are more common in Europe and Asia. The Mondex card is one of the original smart cards, invented in 1990 by NatWest Bank in England. The card allows users to download cash from a bank account to the card via a Mondex-compatible telephone or a card reader attached to a PC, and spend large or small amounts. It can carry five different currencies simultaneously and can be accepted by merchants who have readers installed.

The Octopus card is a rechargeable contactless stored value smart card used in Hong Kong. The card debuted in 1997 as a fare collection system for Hong Kong's mass transit system. Today, it has become the world's most successful stored value smart card. It can be used to pay not only for public transportation, but also to make payments at convenience stores and fast-food restaurants and for parking, and point-of-sale applications such as gas and vending machines. As of January 2007, there were over 14 million Octopus cards in circulation, used to conduct over 12 million transactions a day. The card can be recharged online, over the counter, or via special-purpose "add-value" machines. So far, smart cards have played a limited role in supporting electronic transactions on the fly, where the user is mobile (as in a subway train passenger) and wants to make small payments. However, in the future, smart card technology will be integrated with cell phones, and wireless payment to support mobile e-commerce will become more widespread.

DIGITAL ACCUMULATING BALANCE PAYMENT SYSTEMS

Digital accumulating balance payment systems allow users to make micropayments and purchases on the Web, accumulating a debit balance for which they are billed at the end of the month. Like a utility or phone bill, consumers are expected to pay the entire balance at the end of the month using a checking or credit card

digital accumulating balance payment system
allows users to make micropayments and purchases on the Web, accumulating a debit balance for which they are billed at the end of the month

account. Digital accumulating balance systems are ideal for purchasing intellectual property on the Web such as single music tracks, chapters of books, or articles from a newspaper. such as ringtones and games. Balances accumulate and customers are billed monthly with their regular phone bill. A good example is Valista's PaymentsPlus, a system for accumulating balances for small transactions. PaymentsPlus is used by companies such as AOL, Vodafone, NTT DoCoMo, Tiscali, Wanadoo, and T-Online, among others.

Clickshare takes a different approach. Consumers have one account at a Web site of their choice, and then can use that account to purchase digital content from other Web sites without having to reenter credit card or other personal information. Clickshare has found its greatest acceptance with the online newspaper and publishing industry and has recently signed deals with papers as diverse as the *Chicago Sun-Times, Asian Banker, Lawton (Oklahoma) Constitution,* and *Daily Hampshire Gazette,* and publishers such as Crain Communications and the Globe Pequot Press. It also supplies subscription, authentication, and transaction billing for a variety of major newspapers' subscription Web sites aimed at NFL fans, such as Gannett's Packers Premium and the StarTribune's Purple Plus.

DIGITAL CHECKING PAYMENT SYSTEMS

In December 2004, the Federal Reserve announced that for the first time in history, the number of electronic payment transactions (credit, debit, and other forms of electronic payment) exceeded the number of paper checks. However, the venerable check is not yet moving into retirement. Over 35 billion checks were written in the United States in 2006. **Digital checking payment systems** seek to extend the functionality of existing checking accounts for use as online shopping payment tools.

digital checking payment system seeks to extend the functionality of existing checking accounts for use as online shopping payment tool

PayByCheck's system is based on the consumer's existing checking account. When a consumer wishes to pay by check at a merchant site that offers this service, an online authorization form appears that mimics the appearance of a paper check. The user is prompted to fill in checking account information, including a valid check number, bank routing number, and bank account number. To authorize payment, a user must type his or her full name, and in some instances, if required by the merchant, the last four digits of his or her social security number. The payment information is matched against PayByCheck's various databases containing information on known bad check writers, real-time information from the customer's bank about current bank account status, fraud databases, and an address verification system to verify the customer's name and address. Bio identification in the form of a fingerprint scanner attached to a PC can also be used. PayByCheck then produces a check or electronic debit for the amount of the purchase as indicated on the check, and delivers it to the merchant. The check is deposited by the merchant and routed to the consumer's bank for payment, just like a check written from a checkbook. Digital checking has not been successful so far because of the difficulties of verifying the consumer online.

WIRELESS PAYMENT SYSTEMS

There are approximately 3 billion cell phones in use around the world, and in China, the number of cell phones exceeded 300 million in July 2007, a few more than the entire population of the United States. The United States' cell phone population is now estimated at 250 million. These numbers dwarf the global personal computer population of about 1 billion (TIA, 2007; eMarketer, Inc., 2007). In Japan, more than 95% of households have cell phones.

Use of mobile handsets as payment devices is already well established in Europe, Japan, and South Korea. Japan is arguably the most advanced in terms of providing non-voice services to consumers, that is, real mobile commerce. Japanese cell phones can act as bar code readers, GPS locators, FM radios, voice recorders and analog TV tuners, and purchase things such as train tickets, newspapers, restaurant meals, groceries, books, and a host of common retail goods and services. Three kinds of mobile payments systems are used in Japan, and these provide a glimpse of the future of mobile payments in the United States Japanese cell phones support e-money (stored value systems charged by credit cards or bank accounts), mobile debit cards (tied to personal bank accounts), and mobile credit cards. Japanese cell phones act like mobile wallets, containing a variety of payment mechanisms. Consumers can pay merchants by simply waving the cell phone at a merchant payment device that can accept payments. How do the cell phones communicate with merchants when, say, buying a newspaper at a train station or restaurant meal? Japan's largest phone company, NTT DoCoMo, introduced wireless RFID cell phones and a related payment system (FeliCa) in 2004. Currently 10 million wallet phones are in use in Japan.

In the United States, the cell phone has not yet evolved into a fully capable mobile commerce and payment system. The vast majority of cell phone revenues in the United States (estimated to be $134 billion in 2007) come from voice services, not data, information or gaming services (a mere $10 billion). In the United States, cell phone users mostly download ring tones and pay the phone company on next month's bill. The cell phone in the United States is not connected to the wide network of financial institutions, but instead resides behind the walled garden of the telephone providers. In Europe and Asia, cell phone users can pay for a very wide variety of real goods and services, and there, phones are integrated into a wide array of financial institutions (eMarketer, Inc., 2007). The *Insight on Business* story, *Mobile Payment's Future: WavePayMe, TextPayMe* provides a look at the future of mobile commerce in the United States.

5.7 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 (CheckFree, 2007). In the $12.5 trillion U.S. economy with an $8.7 trillion consumer sector for goods and services, there are a lot of bills to pay. In fact, U.S. households receive by mail over 25 billion bills and statements annually (U.S. Census Bureau, 2007; Flynn, 2005). No one knows for sure,

CHAPTER 8

Ethical, Social, and Political Issues in E-commerce

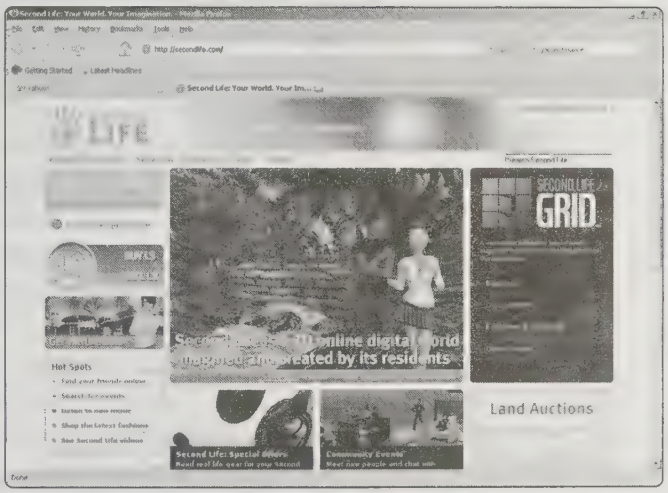
LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Understand why e-commerce raises ethical, social, and political issues.
- Recognize the main ethical, social, and political issues raised by e-commerce.
- Identify a process for analyzing ethical dilemmas.
- Understand basic concepts related to privacy.
- Identify the practices of e-commerce companies that threaten privacy.
- Describe the different methods used to protect online privacy.
- Understand the various forms of intellectual property and the challenges involved in protecting it.
- Understand how governance of the Internet has evolved over time.
- Explain why taxation of e-commerce raises governance and jurisdiction issues.
- Identify major public safety and welfare issues raised by e-commerce.

Second Life Gets a Life:
Discovering Law and Ethics in Virtual Worlds

Second Life is a massively multiplayer online role playing game (MMORPG) experience where upwards of 600,000 active users (and over 5 million unique subscribers) engage in online virtual activities that can range from innocent social chitchat to hustling, buying, selling, and even stealing. With liquidity provided by Linden dollars that can be purchased with real dollars ($1=270 Linden dollars), avatars that you create can buy and sell virtual assets—goods and services—from handbags and cars, to real estate, avatar design, clothing, and accessories service businesses. Some popular services include simulated prostitution, strip clubs, and, not surprisingly, gambling. Second Life commerce generates between $250,000 and $1 million in U.S. dollar revenues each day.



For the most part, players come not to compete with one another, but to entertain themselves, escape their real worlds, and have some fun. Others come in an attempt to make a profit, and a small number come to create mischief. Mischief, so much a part of the real world where law and custom aim to hold it in check, poses an interesting challenge for virtual worlds where there are no laws, and yet where actions taken online can injure people and corporations offline. It's like the Old West, where law and order were not quite established and people sought solutions, looking at times for a strong High Noon sheriff to bring order. Every now and then, the Sheriff sets down the law in Second Life, when its owners declare certain activities illegal and attempt to set up a system of self-regulation (if not quite law).

For instance, many of the assets, goods, and services sold on Second Life do not "belong" to the people who are selling them. You can buy virtual Gucci bags, Ferrari cars (L$ 1,995—what a deal!), Rolex watches, Rayban sunglasses, Prada and Oakley clothes for your avatars, Nike shoes, and Apple iPods. In a small study conducted by several lawyers, of 10 randomly selected virtual stores on Second Life, seven sold knock-off goods that exhibited obvious trademark infringements. Some stores sold nothing but brand-name goods. But because this is all virtual, none of the mentioned trademark owners have thus far brought a lawsuit against residents. As lawyers point out, unless companies actively enforce their trademarks in the face of infringement, they can lose the trademark altogether. From a practical point of view, at some point, nearly all firms will have a virtual presence, and when they seek to develop their trademarks on virtual sites, they will not want to compete with hundreds or thousands of residents selling knockoffs.

In a further sign of emerging legal and ethical issues, six major content creators on Second Life filed a real-world copyright and trademark infringement lawsuit against Thomas Simon, a Queens, New York, resident. Simon allegedly found a flaw in the Second Life program, and used a third-party copy program to make thousands of copies of the creators' products. Included in the alleged theft are avatar clothing, skins and shapes, scripted objects, furniture, and other objects. The plaintiffs did not want to file a lawsuit. They initially sent letters to Simon after having identified him as the owner of the Rase Kenzo avatar. He replied to the plaintiffs in several "drop dead" e-mail messages. The plaintiffs tried to alert Linden Labs by filing copyright notices, filling out support tickets, and filing abuse reports. To complicate matters, the plaintiffs "broke into" Rase Kenzo's skybox to find the evidence of infringement. In the real world, the evidence obtained by unlawful means would be disallowed.

Linden Labs is struggling with issues of governance and ethics on Second Life. It has banned six behaviors: intolerance (including slurs against groups), harassment, assault (including use of software tools to attack people's avatars), disclosure of information about other people's real-world lives, indecency (sexual behavior outside areas rated as mature), and disturbing the peace. Violations prompt warnings, suspension or banishment, enforced by Linden managers. There is no appeal process or due process.

The large-scale trademark and copyright infringements raise concerns about virtual life and real life law and statutes. Stealing in virtual life would seem to parallel stealing in real life. Gambling is another matter. Linden Lab's terms of service ban any illegal activity, but the company itself is not sure whether in-world gambling or prostitution crosses the line. The FBI and federal prosecutors were invited to visit Second Life gambling operations in April 2007, but issued no opinion on the legality of the operation. According to Ginsu Yoon, Vice President of Business Affairs, "It's not always clear to us whether a 3-D simulation of a casino is the same thing as a casino, legally speaking—and it's not clear to the law enforcement authorities we have asked." Even if the law were clear, he said the company would have no way to monitor or prevent in-world gambling, much as law enforcement cannot police every neighborhood poker game or office basketball pool. "There are millions of registered accounts and tens of millions of different objects in Second Life; there is simply no way for us to monitor content prospectively even if we wanted to," Yoon said. "That would be a harder task than pre-monitoring all e-mail sent through Yahoo Mail or Gmail, and no one expects those services to prevent all possible use of e-mail for illegal activity." This sounds like no one is in control, and real-world laws just don't apply, an argument that used to be made by peer-to-peer music sites. Ultimately, the Supreme Court in the real world shut down those music sites because they intentionally established a mechanism to violate copyright laws. In July 2007, Linden Labs decided to outlaw all forms of gambling.

Linden Labs and Second Life have a strong libertarian history. Its founders envisaged Second Life as a self-regulating community where good people could amuse themselves in a fantasy world. Dealing with "griefers," and their growing numbers as evidenced by rapidly expanding abuse complaints at Second Life, suggest that Linden's executives should start thinking about what they have created and how they will police it. If not, real world prosecutors and courts will do it for them. Second Life will have to grow up someday.

SOURCES: "Rapid Trademark Infringement in Second Life Costs Millions, Undermines Future Enforcement," by Benjamin Duranske, Virtuallyblind.com, October 30, 2007; "Second Life Players Bring Virtual Reality to Court," by Emil Steiner, Washingtonpost.com, October 29, 2007; "Second Life Virtual Gamblers Told to Fold," by Mike Musgrove, *Washington Post*, August 1, 2007; "Fantasy Life, Real Law," by Stephanie Ward, *ABA Journal*, March, 2007; "Virtual Vandalism," by Don Clark, *Wall Street Journal*, November 27, 2006.

Determining how to regulate virtual behavior that may have a real-world impact is just one of many ethical, social, and political issues raised by the rapid evolution of the Internet and e-commerce. These questions are not just ethical questions that we as individuals have to answer; they also involve social institutions such as family, schools, and business firms. And these questions have obvious political dimensions because they involve collective choices about how we should live and what laws we would like to live under.

In this chapter, we discuss the ethical, social, and political issues raised in e-commerce, provide a framework for organizing the issues, and make recommendations for managers who are given the responsibility of operating e-commerce companies within commonly accepted standards of appropriateness.

8.1 UNDERSTANDING ETHICAL, SOCIAL, AND POLITICAL ISSUES IN E-COMMERCE

The Internet and its use in e-commerce have raised pervasive ethical, social, and political issues on a scale unprecedented for computer technology. Entire sections of daily newspapers and weekly magazines are devoted to the social impact of the Internet. But why is this so? Why is the Internet at the root of so many contemporary controversies? Part of the answer lies in the underlying features of Internet technology itself, and the ways in which it has been exploited by business firms. Internet technology and its use in e-commerce disrupt existing social and business relationships and understandings.

Consider for instance Table 1.2 (in Chapter 1), which lists the unique features of Internet technology. Instead of considering the business consequences of each unique feature, **Table 8.1** examines the actual or potential ethical, social, and/or political consequences of the technology.

We live in an "information society," where power and wealth increasingly depend on information and knowledge as central assets. Controversies over information are often disagreements over power, wealth, influence, and other things thought to be valuable. Like other technologies, such as steam, electricity, telephones, and television, the Internet and e-commerce can be used to achieve social progress, and for the most part, this has occurred. However, the same technologies can be used to commit crimes, despoil the environment, and threaten cherished social values. Before automobiles, there was very little interstate crime and very little federal jurisdiction over crime. Likewise with the Internet: before the Internet, there was very little "cybercrime."

Many business firms and individuals are benefiting from the commercial development of the Internet, but this development also exacts a price from individuals, organizations, and societies. These costs and benefits must be carefully considered by those seeking to make ethical and socially responsible decisions in this new environment. The question is: How can you as a manager make reasoned judgments about what your firm should do in a number of e-commerce areas—from

TABLE 8.1 UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY AND THEIR POTENTIAL ETHICAL, SOCIAL, AND/OR POLITICAL IMPLICATIONS

E-COMMERCE TECHNOLOGY DIMENSION	POTENTIAL ETHICAL, SOCIAL, AND POLITICAL SIGNIFICANCE
Ubiquity—Internet/Web technology is available everywhere: at work, at home, and elsewhere via mobile devices, anytime.	Work and shopping can invade family life; shopping can distract workers at work, lowering productivity; use of mobile devices can lead to automobile and industrial accidents. Presents confusing issues of "nexus" to taxation authorities.
Global reach—The technology reaches across national boundaries, around the Earth.	Reduces cultural diversity in products; weakens local small firms while strengthening large global firms; moves manufacturing production to low-wage areas of the world; weakens the ability of all nations—large and small—to control their information destiny.
Universal standards—There is one set of technology standards, namely Internet standards.	Increases vulnerability to viruses and hacking attacks worldwide affecting millions of people at once. Increases the likelihood of "information" crime, crimes against systems, and deception.
Richness—Video, audio, and text messages are possible.	A "screen technology" that reduces use of text and potentially the ability to read by focusing instead on video and audio messages. Potentially very persuasive messages possible that may reduce reliance on multiple independent sources of information.
Interactivity—The technology works through interaction with the user.	The nature of interactivity at commercial sites can be shallow and meaningless. Customer e-mails are frequently not read by human beings. Customers do not really "co-produce" the product as much as they "co-produce" the sale. The amount of "customization" of products that occurs is minimal, occurring within predefined platforms and plug-in options.
Information density—The technology reduces information costs, raises quality.	While the total amount of information available to all parties increases, so does the possibility of false and misleading information, unwanted information, and invasion of solitude. Trust, authenticity, accuracy, completeness, and other quality features of information can be degraded. The ability of individuals and organizations to make sense of out of this plethora of information is limited.
Personalization/Customization—The technology allows personalized messages to be delivered to individuals as well as groups.	Opens up the possibility of intensive invasion of privacy for commercial and governmental purposes that is unprecedented.
Social technology—The technology enables user content generation and social networking.	Creates opportunities for cyberbullying, abusive language, and predation; challenges concepts of privacy, fair use, and consent to use posted information; creates new opportunities for surveillance by authorities and corporations into private lives.

securing the privacy of your customer's clickstream to ensuring the integrity of your company's domain name?

A MODEL FOR ORGANIZING THE ISSUES

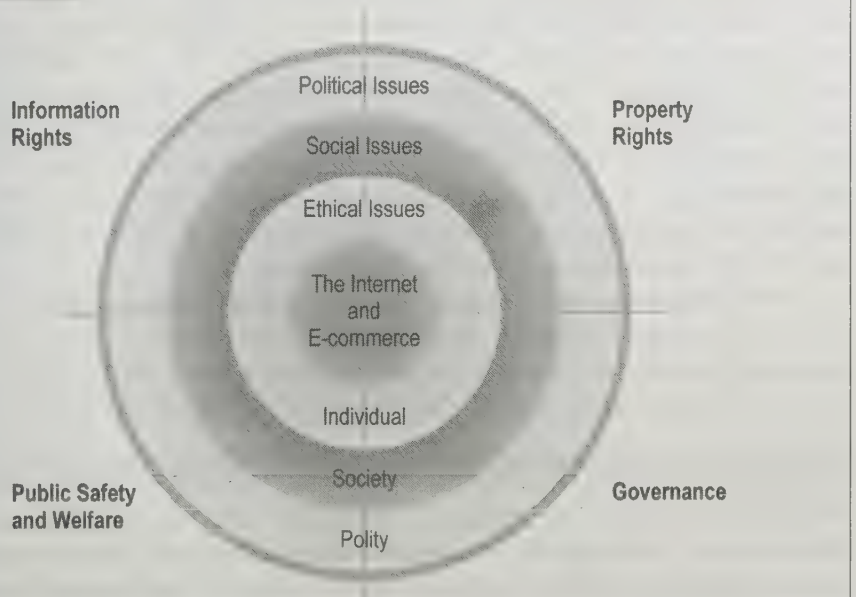
E-commerce—and the Internet—have raised so many ethical, social, and political issues that it is difficult to classify them all, and hence complicated to see their relationship to one another. Clearly, ethical, social, and political issues are interrelated. One way to organize the ethical, social, and political dimensions surrounding e-commerce is shown in **Figure 8.1**. At the individual level, what appears as an ethical issue—"What should I do?"—is reflected at the social and

political levels—"What should we as a society and government do?" The ethical dilemmas you face as a manager of a business using the Web reverberate and are reflected in social and political debates. The major ethical, social, and political issues that have developed around e-commerce over the past nine to ten years can be loosely categorized into four major dimensions: information rights, property rights, governance, and public safety and welfare.

Some of the ethical, social, and political issues raised in each of these areas include the following:

- **Information rights:** What rights to their own personal information do individuals have in a public marketplace, or in their private homes, when Internet technologies make information collection so pervasive and efficient? What rights do individuals have to access information about business firms and other organizations?
- **Property rights:** How can traditional intellectual property rights be enforced in an Internet world where perfect copies of protected works can be made and easily distributed worldwide in seconds?
- **Governance:** Should the Internet and e-commerce be subject to public laws? And if so, what law-making bodies have jurisdiction—state, federal, and/or international?

FIGURE 4.2 THE MORAL DIMENSIONS OF AN INTERNET SOCIETY



The introduction of the Internet and e-commerce impacts individuals, societies, and political institutions. These impacts can be classified into four moral dimensions: property rights, information rights, governance, and public safety and welfare.

- **Public safety and welfare:** What efforts should be undertaken to ensure equitable access to the Internet and e-commerce channels? Should governments be responsible for ensuring that schools and colleges have access to the Internet? Are certain online content and activities—such as pornography and gambling—a threat to public safety and welfare? Should mobile commerce be allowed from moving vehicles?

To illustrate, imagine that at any given moment, society and individuals are more or less in an ethical equilibrium brought about by a delicate balancing of individuals, social organizations, and political institutions. Individuals know what is expected of them, social organizations such as business firms know their limits, capabilities, and roles, and political institutions provide a supportive framework of market regulation, banking, and commercial law that provides sanctions against violators.

Now, imagine we drop into the middle of this calm setting a powerful new technology such as the Internet and e-commerce. Suddenly, individuals, business firms, and political institutions are confronted by new possibilities of behavior. For instance, individuals discover that they can download perfect digital copies of music tracks from Web sites without paying anyone, something that, under the old technology of CDs, would have been impossible. This can be done, despite the fact that these music tracks still "belong" as a legal matter to the owners of the copyright—musicians and record label companies. Then, business firms discover that they can make a business out of aggregating these digital musical tracks—or creating a mechanism for sharing musical tracks—even though they do not "own" them in the traditional sense. This, of course, is the story of Grokster, Kazaa, and Napster described in Chapter 1. The record companies, courts, and Congress were not prepared at first to cope with the onslaught of online digital copying. Courts and legislative bodies will have to make new laws and reach new judgments about who owns digital copies of copyrighted works and under what conditions such works can be "shared." It may take years to develop new understandings, laws, and acceptable behavior in just this one area of social impact. In the meantime, as an individual and a manager, you will have to decide what you and your firm should do in legal "gray" areas, where there is conflict between ethical principles but no clear-cut legal or cultural guidelines. How can you make good decisions in this type of situation?

Before examining the four moral dimensions of e-commerce in greater depth, we will briefly review some basic concepts of ethical reasoning that you can use as a guide to ethical decision making, and provide general reasoning principles about the social and political issues of the Internet that you will face in the future.

BASIC ETHICAL CONCEPTS: RESPONSIBILITY, ACCOUNTABILITY, AND LIABILITY

ethics
the study of principles that individuals and organizations can use to determine right and wrong courses of action

Ethics is at the heart of social and political debates about the Internet. **Ethics** is the study of principles that individuals and organizations can use to determine right and wrong courses of action. It is assumed in ethics that individuals are free moral agents who are in a position to make choices. When faced with alternative courses of action, what is the correct moral choice? Extending ethics from individuals to business firms and even entire societies can be difficult, but it is not impossible. As long as there is

a decision-making body or individual (such as a Board of Directors or CEO in a business firm, or a governmental body in a society), their decisions can be judged against a variety of ethical principles.

If you understand some basic ethical principles, your ability to reason about larger social and political debates will be improved. In western culture, there are three basic principles that all ethical schools of thought share: responsibility, accountability, and liability. **Responsibility** means that as free moral agents, individuals, organizations, and societies are responsible for the actions they take. **Accountability** means that individuals, organizations, and societies should be held accountable to others for the consequences of their actions. The third principle—**liability**—extends the concepts of responsibility and accountability to the area of law. Liability is a feature of political systems in which a body of law is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. **Due process** is a feature of law-governed societies and refers to a process in which laws are known and understood and there is an ability to appeal to higher authorities to ensure that the laws have been applied correctly.

responsibility
as free moral agents, individuals, organizations, and societies are responsible for the actions they take

accountability
individuals, organizations, and societies should be held accountable to others for the consequences of their actions

liability
a feature of political systems in which a body of law is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations

due process
a process in which laws are known and understood and there is an ability to appeal to higher authorities to ensure that the laws have been applied correctly

You can use these concepts immediately to understand some contemporary Internet debates. For instance, consider the *Metro-Goldwyn-Mayer v. Grokster* lawsuit discussed in the case study at the end of Chapter 1. MGM and other studios that joined it in the case argued that because the primary and intended use of Internet P2P file-sharing services such as Grokster, StreamCast, and Kazaa was the swapping of copyright-protected music and video files, the file-sharing services should be held accountable, and shut down. Although Grokster and the other networks acknowledged that the most common use of the software was for illegal digital music file-swapping, they argued that there were substantial, nontrivial uses of the same networks for legally sharing files. They also argued they should not be held accountable for what individuals do with their software, any more than Sony could be held accountable for how people use VCRs, or Xerox for how people use copying machines. In June 2005, the case finally reached the Supreme Court, which ruled that Grokster and other P2P networks could be held accountable for the illegal actions of their users if it could be shown that they intended their software to be used for illegal downloading and sharing, and had marketed the software for that purpose. The court relied on copyright laws to arrive at its decisions, but these laws reflect some basic underlying ethical principles of responsibility, accountability, and liability.

Underlying the *Grokster* Supreme Court decision is a fundamental rejection of the notion that the Internet is an ungoverned "Wild West" environment that cannot be controlled. Under certain defined circumstances, the courts will intervene into the uses of the Internet. No organized civilized society has ever accepted the proposition that technology can flaunt basic underlying social and cultural values. Through all of the industrial and technological developments that have taken place, societies have intervened by means of legal and political decisions to ensure that the technology serves socially acceptable ends without stifling the positive consequences of innovation and wealth creation. The Internet in this sense is no different, and we can expect societies around the world to exercise more regulatory control over the Internet and e-commerce in an effort to arrive at a new balance between innovation and wealth creation, on the one hand, and other socially desirable objectives on the

other. This is a difficult balancing act, and reasonable people will arrive at different conclusions.

ANALYZING ETHICAL DILEMMAS

dilemma
a situation in which there are at least two diametrically opposed actions, each of which supports a desirable outcome

Ethical, social, and political controversies usually present themselves as dilemmas. A **dilemma** is a situation in which there are at least two diametrically opposed actions, each of which supports a desirable outcome. When confronted with a situation that seems to present an ethical dilemma, how can you analyze and reason about the situation? The following is a five-step process that should help:

1. **Identify and clearly describe the facts.** Find out who did what to whom, and where, when, and how. In many instances, you will be surprised at the errors in the initially reported facts, and often you will find that simply getting the facts straight helps define the solution. It also helps to get the opposing parties involved in an ethical dilemma to agree on the facts.
2. **Define the conflict or dilemma and identify the higher-order values involved.** Ethical, social, and political issues always reference higher values. Otherwise, there would be no debate. The parties to a dispute all claim to be pursuing higher values (e.g., freedom, privacy, protection of property, and the free enterprise system). For example, supporters of the use of advertising networks such as DoubleClick argue that the tracking of consumer movements on the Web increases market efficiency and the wealth of the entire society. Opponents argue this claimed efficiency comes at the expense of individual privacy, and advertising networks should cease their activities or offer Web users the option of not participating in such tracking.
3. **Identify the stakeholders.** Every ethical, social, and political issue has stakeholders: players in the game who have an interest in the outcome, who have invested in the situation, and usually who have vocal opinions. Find out the identity of these groups and what they want. This will be useful later when designing a solution.
4. **Identify the options that you can reasonably take.** You may find that none of the options satisfies all the interests involved, but that some options do a better job than others. Sometimes, arriving at a "good" or ethical solution may not always be a balancing of consequences to stakeholders.
5. **Identify the potential consequences of your options.** Some options may be ethically correct, but disastrous from other points of view. Other options may work in this one instance, but not in other similar instances. Always ask yourself, "What if I choose this option consistently over time?"

Once your analysis is complete, you can refer to the following well-established ethical principles to help decide the matter.

CANDIDATE ETHICAL PRINCIPLES

Although you are the only one who can decide which ethical principles you will follow and how you will prioritize them, it is helpful to consider some ethical principles with deep roots in many cultures that have survived throughout recorded history:

- **The Golden Rule:** Do unto others as you would have them do unto you. Putting yourself into the place of others and thinking of yourself as the object of the decision can help you think about fairness in decision making.
- **Universalism:** If an action is not right for all situations, then it is not right for any specific situation (Immanuel Kant's categorical imperative). Ask yourself, "If we adopted this rule in every case, could the organization, or society, survive?"
- **Slippery Slope:** If an action cannot be taken repeatedly, then it is not right to take at all (Descartes' rule of change). An action may appear to work in one instance to solve a problem, but if repeated, would result in a negative outcome. In plain English, this rule might be stated as "once started down a slippery path, you may not be able to stop."
- **Collective Utilitarian Principle:** Take the action that achieves the greater value for all of society. This rule assumes you can prioritize values in a rank order and understand the consequences of various courses of action.
- **Risk Aversion:** Take the action that produces the least harm, or the least potential cost. Some actions have extremely high failure costs of very low probability (e.g., building a nuclear generating facility in an urban area) or extremely high failure costs of moderate probability (speeding and automobile accidents). Avoid the high-failure cost actions and choose those actions whose consequences would not be catastrophic, even if there were a failure.
- **No Free Lunch:** Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise. (This is the ethical "no free lunch" rule.) If something someone else has created is useful to you, it has value and you should assume the creator wants compensation for this work.
- **The *New York Times* Test (Perfect Information Rule):** Assume that the results of your decision on a matter will be the subject of the lead article in the *New York Times* the next day. Will the reaction of readers be positive or negative? Would your parents, friends, and children be proud of your decision? Most criminals and unethical actors assume imperfect information, and therefore they assume their decisions and actions will never be revealed. When making decisions involving ethical dilemmas, it is wise to assume perfect information markets.
- **The Social Contract Rule:** Would you like to live in a society where the principle you are supporting would become an organizing principle of the entire society?

For instance, you might think it is wonderful to download illegal copies of music tracks, but you might not want to live in a society that did not respect property rights, such as your property rights to the car in your driveway, or your rights to a term paper or original art.

None of these rules is an absolute guide, and there are exceptions and logical difficulties with all of them. Nevertheless, actions that do not easily pass these guidelines deserve some very close attention and a great deal of caution because the appearance of unethical behavior may do as much harm to you and your company as the actual behavior.

Now that you have an understanding of some basic ethical reasoning concepts, let's take a closer look at each of the major types of ethical, social, and political debates that have arisen in e-commerce.

8.2 PRIVACY AND INFORMATION RIGHTS

privacy
the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state

information privacy
includes both the claim that certain information should not be collected at all by governments or business firms, and the claim of individuals to control the use of whatever information that is collected about them

Privacy is the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Privacy is a girder supporting freedom: Without the privacy required to think, write, plan, and associate independently and without fear, social and political freedom is weakened, and perhaps destroyed. **Information privacy** is a subset of privacy. The right to information privacy includes both the claim that certain information should not be collected at all by governments or business firms, and the claim of individuals to control the use of whatever information that is collected about them. Individual control over personal information is at the core of the privacy concept.

Due process also plays an important role in defining privacy. The best statement of due process in record keeping is given by the Fair Information Practices doctrine developed in the early 1970s and extended to the online privacy debate in the late 1990s (described later in this section).

There are two kinds of threats to individual privacy posed by the Internet. One threat originates in the private sector and concerns how much personal information is collected by commercial Web sites and how it will be used. A second threat originates in the public sector and concerns how much personal information federal, state, and local government authorities collect, and how they use it.

Privacy claims—and thinking about privacy—mushroomed in the United States at the end of the nineteenth century as the technology of photography and tabloid journalism enabled the invasion of the heretofore private lives of wealthy industrialists. For most of the twentieth century, however, privacy thinking and legislation focused on restraining the government from collecting and using personal information. With the explosion in the collection of private personal information by Web-based marketing firms since 1995, privacy concerns are increasingly directed toward restraining the activities of private firms in the collection and use of information on the Web. Claims to privacy are also involved at the workplace. Millions of employees are subject to various forms of electronic surveillance that in many cases is enhanced by firm intranets and Web technologies. For instance, the majority of U.S. companies monitor which Web sites their workers visit, as well as employee e-mail and instant messages. Employee posts on message boards and blogs are also coming under scrutiny (Vaughan, 2007).

In general, the Internet and the Web provide an ideal environment for both business and government to invade the personal privacy of millions of users on a scale unprecedented in history. Perhaps no other recent issue has raised as much widespread social and political concern as protecting the privacy of over 175–200 million Web users in the United States alone. The major ethical issues related to e-commerce and privacy include the following: Under what conditions should we

site privacy policies, has not been too successful. But ISPs and independent software companies now provide a host of tools that work wonders and are easy to use. AOL recently announced that it would offer a "Do Not Track" service that will link consumers directly to opt-out lists offered by the large advertising networks. The open source browser Firefox and Internet Explorer 6.0/7 have effective pop-up and image blockers. Google, Yahoo, MSN, and AOL also offer toolbars that provide similar help. Adoption rates of cookie blockers and anti-spyware software are increasing as software makers such as Symantec make them available as a part of their software suites that install automatically. For instance, a recent survey found that anti-virus, anti-spyware, and firewall software are used by over 80% of U.S. adult Internet users, and that over two-thirds had configured their browser or operating system to block pop-ups, reject cookies or block specific Web sites. Even if these estimates are off by 50%, a significant number of ads are not actually being shown to consumers.

All these consumer self-help activities have traditional Web advertisers worried. What if consumers rejected the idea of pop-up ads, tracking their behavior, and storing all this information about them? What if consumers did not buy into the "free Internet with ads" deal? What if 50% of Internet users adopted ISP-provided privacy protection or bought their equivalents on the market? While Internet advertisers have pretty much blocked effective legislation in Washington that would preserve privacy, and while their industry associations have quite clearly failed to bring about meaningful self-regulation, the market has responded by providing consumers with some powerful tools for protecting their own privacy.

SOURCES: "Are Facebooks Social Ads Illegal?", by Saul Hansell, *New York Times*, November 8, 2007; "Tracking of Web Use by Marketers Gains Favor," by Louise Story, *New York Times*, November 5, 2007; "The Higher Value of Eyeballs," by Louise Story, *New York Times*, November 5, 2007; "AOL's 'Do Not Track' Effect, " by Ben Macklin, eMarketer, Inc., November 3, 2007; "Privacy Groups Seek 'Do Not Track' Web List," Reuters, November 1, 2007; "F.T.C. to Review Online Ads and Privacy," by Louise Story, *New York Times*, November 1, 2007; "Online Privacy? For Young People, That's Old-School," by Janet Kornbum, *USA Today*, October 22, 2007; "Firm Mines Offline Data to Target Online Ads," by Kevin J. Delaney and Emily Steel, *Wall Street Journal*, October 17, 2007; "Consumers Have False Sense of Security About Online Privacy - Actions Inconsistent with Attitudes," TRUSTe.org, December 6, 2006.

8.3 INTELLECTUAL PROPERTY RIGHTS

> Congress shall have the power to "promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."
>
> —Article I, Section 8, Constitution of the United States, 1788.

Next to privacy, the most controversial ethical, social, and political issue related to e-commerce is the fate of intellectual property rights. Intellectual property encompasses all the tangible and intangible products of the human mind. As a general rule, in the United States, the creator of intellectual property owns it. For instance, if you personally create an e-commerce site, it belongs entirely to you, and you have

exclusive rights to use this "property" in any lawful way you see fit. But the Internet potentially changes things. Once intellectual works become digital, it becomes difficult to control access, use, distribution, and copying. These are precisely the areas that intellectual property seeks to control.

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

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

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

TYPES OF INTELLECTUAL PROPERTY PROTECTION

There are three main types of intellectual property protection: copyright, patent, and trademark law. In the United States, the development of intellectual property law begins in the U.S. Constitution in 1788, which mandated Congress to devise a system of laws to promote "the progress of science and the useful arts." Congress passed the first copyright law in 1790 to protect original written works for a period of 14 years, with a 14-year renewal if the author was still alive. Since then, the idea of copyright has been extended to include music, films, translations, photographs, and most recently (1998), the designs of vessels under 200 feet (Fisher, 1999). The copyright law has been amended (mostly extended) 11 times in the last 40 years.

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

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

COPYRIGHT: THE PROBLEM OF PERFECT COPIES AND ENCRYPTION

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

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

In 1998, Congress extended the period of copyright protection for an additional 20 years, for a total of 95 years for corporate-owned works, and life plus 70 years of protection for works created by individuals (the Copyright Term Extension Act, also known as CETA). In *Eldred v. Ashcroft*, the Supreme Court ruled on January 16, 2003, that CETA was constitutional, over the objections of groups arguing that Congress had given copyright holders a permanent monopoly over the expression of ideas, which ultimately would work to inhibit the flow of ideas and creation of new works by making existing works too expensive (Greenhouse, 2003a). Librarians, academics, and others who depend on inexpensive access to copyrighted material opposed the legislation.

Since the first federal Copyright Act of 1790, the congressional intent behind copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work. Most industrial nations have their own copyright laws, and there are several international conventions and bilateral agreements through which nations coordinate and enforce their laws.

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

Copyright protection is clear-cut: it protects against copying of entire programs or their parts. Damages and relief are readily obtained for infringement. The drawback

to copyright protection is that the underlying ideas behind a work are not protected, only their expression in a work. A competitor can view the source code on your Web site to see how various effects were created and then reuse those techniques to create a different Web site without infringing on your copyright.

Look and Feel

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

Fair Use Doctrine

Copyrights, like all rights, are not absolute. There are situations where strict copyright observance could be harmful to society, potentially inhibiting other rights such as the right to freedom of expression and thought. As a result, the doctrine of fair use has been created. The **doctrine of fair use** permits teachers and writers to use copyrighted materials without permission under certain circumstances. **Table 8.9** describes the five factors that courts consider when assessing what constitutes fair use.

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

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

What constitutes fair use has been at issue in a number of recent cases, including the Google Book Search Project described in the case study at the end of the chapter, and in several recent lawsuits. In *Kelly v. ArribaSoft* (2003) and *Perfect 10, Inc. v. Amazon.com, Inc.* (2007), the federal Circuit Court of Appeals for the 10th circuit held that the display of thumbnail images in response to search requests constituted fair use. A similar result was reached by the district court for the District of Nevada with

TABLE 8.9 FAIR USE CONSIDERATIONS TO COPYRIGHT PROTECTIONS

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

respect to Google's storage and display of Web sites from cache memory, in *Field v. Google, Inc.* (2006). In all of these cases, the courts accepted the argument that caching the material and displaying it in response to a search request was not only a public benefit, but also a form of marketing of the material on behalf of its copyright owner, thereby enhancing the material's commercial value. Fair use is also at issue in the lawsuit filed by Viacom against Google and YouTube in March 2007, described further in the next section.

The Digital Millennium Copyright Act of 1998

The Digital Millennium Copyright Act (DMCA) of 1998 is the first major effort to adjust the copyright laws to the Internet age. This legislation was the result of a confrontation between the major copyright holders in the United States (publishing, sheet music, record label, and commercial film industries), ISPs, and users of copyrighted materials such as libraries, universities, and consumers. While social and political institutions are sometimes thought of as "slow" and the Internet as "fast," in this instance, powerful groups of copyright owners anticipated Web music services such as Napster by several years. Napster was formed in 1999, but work by the World Intellectual Property Organization—a worldwide body formed by the major copyright—holding nations of North America, Europe, and Japan—began in 1995. **Table 8.10** summarizes the major provisions of the DMCA.

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

The penalties for willfully violating the DMCA include restitution to the injured parties of any losses due to infringement. Criminal remedies are available to federal prosecutors that include fines up to $500,000 or five years imprisonment for a first offense, and up to $1 million in fines and 10 years in prison for repeat offenders. These are serious remedies.

The DMCA attempts to answer two vexing questions in the Internet age. First, how can society protect copyrights online when any practical encryption scheme imaginable can be broken by hackers and the results distributed worldwide? Second, how can society control the behavior of thousands of ISPs, who often host infringing

TABLE 8.10 THE DIGITAL MILLENNIUM COPYRIGHT ACT

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

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

Web sites, or who provide Internet service to individuals who are routine infringers? ISPs claim to be like telephone utilities—just carrying messages—and they do not want to put their users under surveillance or invade the privacy of users. The DMCA recognizes that ISPs have some control over how their customers use their facilities.

The DMCA implements a World Intellectual Property Organization (WIPO) treaty of 1996, which declares it illegal to make, distribute, or use devices that circumvent technology-based protections of copyrighted materials, and attaches stiff fines and prison sentences for violations. WIPO is an organization within the United Nations. Recognizing that these provisions alone cannot stop hackers from devising circumventions, the DMCA makes it difficult for such inventors to reap the fruits of their labors by making the ISPs (including universities) responsible and accountable for hosting Web sites or providing services to infringers once the ISP has been notified. ISPs are not required to intrude on their users. However, when copyright holders inform the ISP that a hosted site or individual users are infringing, they must "take down" the site immediately to avoid liability and potential fines. ISPs must also inform their subscribers of their copyright management policies. Copyright owners can subpoena the personal identities of any infringers using an ISP. There are important limitations on these ISP prohibitions that are mostly concerned with the transitory caching of materials for short periods without the knowledge of the ISP. However, should the ISP be deriving revenues from the infringement, it is as liable as the infringer, and is subject to the same penalties.

Title I of the DMCA provides a partial answer to the dilemma of hacking. It is probably true that skilled hackers can easily break any usable encryption scheme, and

the means to do so on a large scale through distribution of the decryption programs already exists. The WIPO provisions accept this possibility and simply make it illegal to do so, or to disseminate, or to enable such dissemination or even storage and transmission of decrypted products or tools. These provisions put large ISPs on legal notice.

There are a number of exceptions to the strong prohibitions against defeating a copyright protection scheme outlined above. There are exceptions for libraries to examine works for adoption, for reverse engineering to achieve interoperability with other software, for encryption research, for privacy protection purposes, and for security testing. Many companies, such as YouTube, Google, and MySpace have latched on the provision of the DMCA that relates to removing infringing material upon request of the copyright owner as a "safe harbor" that precludes them from being held responsible for copyright infringement. This position is currently being tested in a $1 billion lawsuit brought by Viacom against Google and YouTube for willful copyright infringement, and by Vivendi's Universal Music Group against the News Corp.'s MySpace. These lawsuits are interesting because, unlike efforts against individuals accused of file-sharing, or offshore renegade outfits such as Kazaa, they pit large established corporate institutions against one another.

In the Viacom case, Viacom alleges that YouTube and Google engaged in massive copyright infringement by deliberately building up a library of infringing works to draw traffic to the YouTube site and enhance its commercial value. In response, Google and YouTube claim that they are protected by the DMCA's safe harbor and fair use, and that it is often impossible to know whether a video is infringing or not. YouTube also does not display ads on pages where consumers can view videos unless it has an agreement with the content owner. In October 2007, Google announced a filtering system aimed at addressing the problem. It requires content owners to give Google a copy of their content so Google can load it into an auto-identification system. The copyright owner can specify whether it will allow others to post the material. Then after a video is uploaded to YouTube, the system attempts to match it with its database of copyrighted material, and removes any unauthorized material. Whether content owners will be satisfied with this system is unknown, particularly since guidelines issued by a coalition of major media and Internet companies with respect to the handling of copyrighted videos on user-generated Web sites calls for the use of filtering technology that can block infringing material before it is posted online (Helft and Fabrikant, 2007; Gentile, 2007; Swartz, 2007).

PATENTS: BUSINESS METHODS AND PROCESSES

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

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

A **patent** grants the owner a 20-year exclusive monopoly on the ideas behind an invention. The congressional intent behind patent law was to ensure that inventors of

new machines, devices, or industrial methods would receive the full financial and other rewards of their labor and yet still make widespread use of the invention possible by providing detailed diagrams for those wishing to use the idea under license from the patent's owner. Patents are obtained from the United States Patent and Trademark Office (USPTO), created in 1812. Obtaining a patent is much more difficult and time-consuming than obtaining copyright protection (which is automatic with the creation of the work). Patents must be formally applied for, and the granting of a patent is determined by Patent Office examiners who follow a set of rigorous rules. Ultimately, federal courts decide when patents are valid and when infringement occurs.

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

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

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

The danger of patents is that they stifle competition by raising barriers to entry into an industry. Patents force new entrants to pay licensing fees to incumbents, and thus slow down the development of technical applications of new ideas by creating lengthy licensing applications and delays.

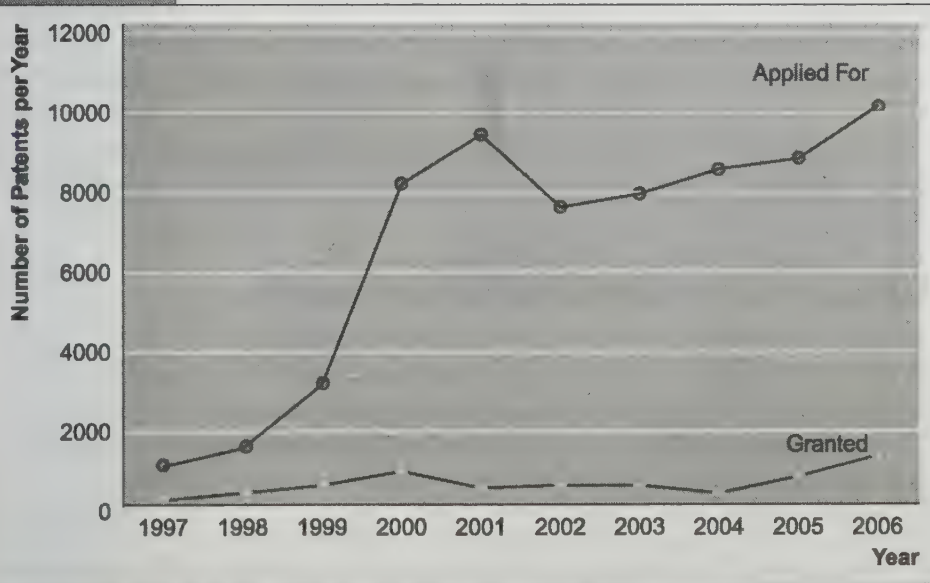
E-commerce Patents

Much of the Internet's infrastructure and software was developed under the auspices of publicly funded scientific and military programs in the United States and Europe. Unlike

Samuel F. B. Morse, who patented the idea of Morse code and made the telegraph useful, most of the inventions that make the Internet and e-commerce possible were not patented by their inventors. The early Internet was characterized by a spirit of worldwide community development and sharing of ideas without consideration of personal wealth (Winston, 1998). This early Internet spirit changed in the mid-1990s with the commercial development of the World Wide Web.

In 1998, a landmark legal decision, *State Street Bank & Trust v. Signature Financial Group, Inc.*, paved the way for business firms to begin applying for "business methods" patents. In this case, a Federal Circuit Court of Appeals upheld the claims of Signature Financial to a valid patent for a business method that allows managers to monitor and record financial information flows generated by a partner fund. Previously, it was thought business methods could not be patented. However, the court ruled there was no reason to disallow business methods from patent protection, or any "step by step process, be it electronic or chemical or mechanical, [that] involves an algorithm in the broad sense of the term" (*State Street Bank & Trust Co. v. Signature Financial Group*, 1998). The State Street decision led to an explosion in applications for e-commerce "business methods" patents, with over 10,000 in 2006 (see **Figure 8.3**). Note that the overall number of patents filed has also increased dramatically, from about 237,000 in 1995 to almost 444,000 in 2006.

FIGURE 8.3 INTERNET AND E-COMMERCE BUSINESS METHODS PATENTS



Bolstered by the 1998 *State Street Bank* decision, patents on computer-related business methods increased exponentially from 1998 when 1,337 applications were filed, to 2001, when 9,288 applications were submitted. During the period 2002–2005, applications dropped off somewhat and remained relatively steady at around 7,500–8,500 per year, but in 2006, they increased significantly again, to over 10,000 applications.

SOURCE: Based on data from U.S. Patent and Trademark Office, 2007.

Table 8.11 lists some of the better-known, controversial e-commerce patents. Reviewing these, you can understand the concerns of commentators and corporations. Some of the patent claims are very broad (for example, "name your price" sales methods), have historical precedents in the pre-Internet era (shopping carts), and seem "obvious" (one-click purchasing). Critics of online business methods patents argue that the Patent Office has been too lenient in granting such patents and that in most instances, the supposed inventions merely copy pre-Internet business methods and thus do not constitute "inventions" (Harmon, 2003; Thurm, 2000; Chiappetta, 2001). The Patent Office argues, on the contrary, that its Internet inventions staff is composed of engineers, lawyers, and specialists with many years of experience with Internet and network technologies, and that it consults with outside technology experts before granting patents. To complicate matters, the European Patent Convention and the patent laws of most European countries do not recognize business methods per se unless the method is implemented through some technology (Takenaka, 2001).

Patent Reform

Issues related to business method patents, patent "trolls" (companies such as Acacia Technologies that buy up broadly-worded patents on a speculative basis and then use them to threaten companies that are purportedly violating the patent) and confusing legal decisions have led to increasing calls for patent reform over the last few years, particularly by companies in the technology sector. In September 2007, the House of Representatives passed its version of a patent reform bill that includes provisions that change the patent system from a "first to invent" system to a "first to file" system, change the way damages for patent infringement are calculated, provide a new way to challenge patents out of court, limit where patent suits can be filed (to prevent suits from being filed in districts that have a reputation for being more favorable), and impose heightened standards for a finding of willful infringement. Whether the bill will ultimately be enacted into law, and if so, its final form, is unknown as of this writing (Broache, 2007).

TRADEMARKS: ONLINE INFRINGEMENT AND DILUTION

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

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

Trademark law is a form of intellectual property protection for **trademarks**—a mark used to identify and distinguish goods and indicate their source. Trademark protections exist at both the federal and state levels in the United States. The purpose of trademark law is twofold. First, the trademark law protects the public in the marketplace by ensuring that it gets what it pays for and wants to receive. Second, trademark law protects the owner—who has spent time, money, and energy bringing

TABLE 8.11 SELECTED E-COMMERCE PATENTS

COMPANY	SUBJECT	UPDATE
Leon Stambler	Secure communications	Private inventor with seven patents (1992–1998) covering creation of an authentication code to be used in electronic communications. In 2003, a Delaware jury found that RSA Security and VeriSign did not infringe on the patents. Stambler's appeal to the U.S. Court of Appeals for the Federal Circuit was rejected in February 2005.
Amazon	One-click purchasing	Amazon attempted to use patent originally granted to it in 1999 to force changes to Barnes & Noble's Web site, but a federal court overturned a previously issued injunction. Eventually settled out of court. In September 2007, a USPTO panel rejected most of the patent because of evidence another patent predated it, sending it back to the patent examiner for reconsideration.
Eolas Technologies	Embedding interactive content in a Web site	Eolas Technologies, a spin-off of the University of California, obtained patent in 1998. Eolas filed suit against Microsoft in 1999 for infringing the patent in Internet Explorer and was award a $520 million judgment in 2003. Decision was partially reversed in 2005, and sent back to district court for a new trial. The patent was reaffirmed in September 2005 by the USPTO. In August 2007, Eolas and Microsoft finally settled the suit on undisclosed terms.
Priceline	Buyer-driven "name your price" sales	Originally invented by Walker Digital, an intellectual property laboratory, and then assigned to Priceline. Granted by the USPTO in 1999. Shortly thereafter, Priceline sued Microsoft and Expedia for copying its patented business method. Expedia settled and agreed to pay a royalty in 2001.
Sightsound	Music downloads	Sightsound won a settlement in 2004 against Bertelsmann subsidiaries CDNow and N2K music sites for infringing its patent.
Akamai	Internet content delivery Global Hosting System	A broad patent granted in 2000 covering techniques for expediting the flow of information over the Internet. Akamai sued Digital Island (subsequently acquired Cable & Wireless) for violating the patent and, in 2001, a jury found in its favor. In 2004, Akamai accepted a damages payment to finally settle the suit.
DoubleClick	Dynamic delivery of online advertising	The patent underlying DoubleClick's business of online banner ad delivery, originally granted in 2000. DoubleClick sued competitors 24/7 Media and L90 for violating the patent and ultimately reached a settlement with them.
Overture	Pay for performance search	System and method for influencing position on search result list generated by computer search engine, granted in 2001. Competitor FindWhat.com sued Overture, charging that patent was obtained illegally; Overture countered by suing both FindWhat and Google for violating patent. Google agreed to pay a license fee to Overture in 2004 to settle the suit, and the lawsuit with FindWhat resulted in a hung jury in 2005, with both sides claiming victory.
Acacia Technologies	Streaming video media transmission	Patents for the receipt and transmission of streaming digital audio and or video content originally granted to founders of Greenwich Information Technologies in 1990s. Patents were purchased by Acacia, a firm founded solely to enforce the patents, in 2001. Acacia has subsequently secured dozens of licenses.
Soverain Software	Purchase technology	The so-called "shopping cart" patent for network-based systems. Originally owned by Open Markets, then Divine Inc., and now Soverain. Soverain filed suit against Amazon for patent infringement in 2004; Amazon settled for $40 million in August 2005.
MercExchange (Thomas Woolston)	Auction technology	Patents on person-to-person auctions and database search, originally granted in 1995. eBay ordered to pay $25 million in 2003 for infringing on patent. In July 2007, the U.S. district court denied a motion for permanent patent injunction against eBay using the "Buy It Now" feature, and moved to the final stages of allowing the damages award to be paid. Issues related to a second patent were deferred pending a USPTO office reexamination.
Google	Search technology	Google PageRank patent was filed in 1998 and granted in 2001.

the product to the marketplace—against piracy and misappropriation. Trademarks have been extended from single words to pictures, shapes, packaging, and colors. Some things may not be trademarked: common words that are merely descriptive ("clock"), flags of states and nations, immoral or deceptive marks, or marks belonging to others. Federal trademarks are obtained, first, by use in interstate commerce, and second, by registration with the USPTO. Trademarks are granted for a period of ten years, and can be renewed indefinitely.

Disputes over federal trademarks involve establishing infringement. The test for infringement is twofold: market confusion and bad faith. Use of a trademark that creates confusion with existing trademarks causes consumers to make market mistakes, or misrepresents the origins of goods is an infringement. In addition, the intentional misuse of words and symbols in the marketplace to extort revenue from legitimate trademark owners ("bad faith") is proscribed.

In 1995, Congress passed the Federal Trademark Dilution Act, which created a federal cause of action for dilution of famous marks. This legislation dispenses with the test of market confusion (although that is still required to claim infringement), and extends protection to owners of famous trademarks against **dilution**, which is defined as any behavior that would weaken the connection between the trademark and the product. Dilution occurs through blurring (weakening the connection between the trademark and the goods) and tarnishment (using the trademark in a way that makes the underlying products appear unsavory or unwholesome).

dilution
any behavior that would weaken the connection between the trademark and the product

Trademarks and the Internet

The rapid growth and commercialization of the Internet have provided unusual opportunities for existing firms with distinctive and famous trademarks to extend their brands to the Internet. These same developments have provided malicious individuals and firms the opportunity to squat on Internet domain names built upon famous marks, as well as attempt to confuse consumers and dilute famous or distinctive marks (including your personal name or a movie star's name). The conflict between legitimate trademark owners and malicious firms was allowed to fester and grow because Network Solutions Inc. (NSI), originally the Internet's sole agency for domain name registration for many years, had a policy of "first come, first served." This meant anyone could register any domain name that had not already been registered, regardless of the trademark status of the domain name. NSI was not authorized to decide trademark issues (Nash, 1997).

In response to a growing number of complaints from owners of famous trademarks who found their trademark names being appropriated by Web entrepreneurs, Congress passed the **Anticybersquatting Consumer Protection Act (ACPA)** in November 1999. The ACPA creates civil liabilities for anyone who attempts in bad faith to profit from an existing famous or distinctive trademark by registering an Internet domain name that is identical, confusingly similar, or "dilutive" of that trademark. The Act does not establish criminal sanctions. The Act proscribes using "bad faith" domain names to extort money from the owners of the existing trademark (**cybersquatting**), or using the bad faith domain to divert Web

Anticybersquatting Consumer Protection Act (ACPA)
creates civil liabilities for anyone who attempts in bad faith to profit from an existing famous or distinctive trademark by registering an Internet domain name that is identical, or confusingly similar, or "dilutive" of that trademark

cybersquatting
involves the registration of an infringing domain name, or other Internet use of an existing trademark, for the purpose of extorting payments from the legitimate owners

CHALLENGE: BALANCING THE PROTECTION OF PROPERTY WITH OTHER VALUES

In the areas of copyright, patent law, and trademark law, societies have moved quickly to protect intellectual property from challenges posed by the Internet. In each of these areas, traditional concepts of intellectual property have not only been upheld, but often strengthened. The DMCA seems to restrict journalists and academics from even accessing copyrighted materials if they are encrypted, a protection not true of traditional documents (which are rarely encrypted anyway). Patents have been extended to Internet business methods, and trademarks are more strongly protected than ever because of fears of cybersquatting. In the early years of e-commerce, many commentators believed that Internet technology would sweep away the powers of corporations to protect their property (Dueker, 1996). The case of Napster and digital music files was a powerful example of how a new technology could disrupt an entrenched business model and an entire industry. In the case of Napster, though, the industry won in court suits and forced Napster's demise. Score one for the industry. Napster was quickly replaced by a newer technology (true peer-to-peer networks). Score one for file swappers. However, the U.S. Supreme Court and courts in Australia have found Grokster and other P2P networks liable for the infringement they enable. Australian courts ordered Sharman Network's P2P network software to track over 3,000 words (author and song names) and remove them from their network. In November 2005, Grokster shut down entirely as part of a legal settlement with the record industry, and paid $50 million in damages (McBride, 2005). Advantage: industry.

It is apparent that corporations have some very powerful legal tools for protecting their digital properties. By 2007, the record industry had filed over 25,000 lawsuits for sharing files (Associated Press, 2007). In addition, there are five arbitration panels established to hear trademark disputes: WIPO, ICANN, the National Arbitration Forum (Minneapolis), eResolutions Consortium (Amherst, Massachusetts), and C.P.R. Institute for Dispute Resolutions in New York. The difficulty now may be in going too far to protect the property interests of the powerful and the rich, preventing parody sites or parody content from receiving wide distribution and recognition, and in this sense interfering with the exercise of First Amendment guarantees of freedom of expression.

8.4 GOVERNANCE

governance
has to do with social control: Who will control e-commerce, what elements will be controlled, and how the controls will be implemented

Governance has to do with social control: Who will control the Internet? Who will control the processes of e-commerce, the content, and the activities? What elements will be controlled, and how will the controls be implemented? A natural question arises and needs to be answered: "Why do we as a society need to 'control' e-commerce?" Because e-commerce and the Internet are so closely intertwined (though not identical), controlling e-commerce also involves regulating the Internet.

WHO GOVERNS E-COMMERCE AND THE INTERNET?

Governance of both the Internet and e-commerce has gone through four stages. **Table 8.13** summarizes these stages in the evolution of e-commerce governance.

TABLE 8.13 THE EVOLUTION OF GOVERNANCE OF E-COMMERCE

INTERNET GOVERNANCE PERIOD	DESCRIPTION
Government Control Period 1970–1994	DARPA and the National Science Foundation control the Internet as a fully government-funded program.
Privatization 1995–1998	Network Solutions Inc. is given a monopoly to assign and track high-level Internet domains. Backbone is sold to private telecommunications companies. Policy issues are not decided.
Self-Regulation 1995–present	President Clinton and the Department of Commerce encourage the creation of a semiprivate body, the Internet Corporation for Assigning Numbers and Names (ICANN), to deal with emerging conflicts and establish policies. ICANN currently holds a contract with the Department of Congress to govern some aspects of the Internet.
Governmental Regulation 1998–present	Executive, legislative, and judicial bodies worldwide begin to implement direct controls over the Internet and e-commerce.

Prior to 1995, the Internet was a government program. Beginning in 1995, private corporations were given control of the technical infrastructure as well as the process of granting IP addresses and domain names. However, the NSI monopoly created in this period did not represent international users of the Internet, and was unable to cope with emerging public policy issues such as trademark and intellectual property protection, fair policies for allocating domains, and growing concerns that a small group of firms were benefiting from growth in the Internet.

In 1995, President Clinton, using funds from the Department of Commerce, encouraged the establishment of an international body called the Internet Corporation for Assigned Names and Numbers (ICANN) that hopefully could better represent a wider range of countries and a broad range of interests, and begin to address emerging public policy issues. ICANN was intended to be an Internet/e-commerce industry self-governing body, not another government agency.

The explosive growth of the Web and e-commerce created a number of issues over which ICANN had no authority. Content issues such as pornography, gambling, and offensive written expressions and graphics, along with commercial issue of intellectual property protection, ushered in the current era of growing governmental regulation of the Internet and e-commerce throughout the world. Currently, we are in a mixed-mode policy environment where self-regulation through a variety of Internet policy and technical bodies co-exists with limited government regulation.

Today, ICANN remains in charge of the domain name system that translates domain names (such as www.company.com) into IP addresses. It has subcontracted

the work of maintaining the databases of the domain registries to several private corporations. The U.S. government controls the "A-root" server. However, these arrangements are increasingly challenged by other countries, including China, Russia, Saudi Arabia, and most of the European Union, all of whom want the United States to give up control over the Internet to an international body such as the International Telecommunication Union (ITU) (a UN agency). In November 2005, an Internet Summit sponsored by the ITU agreed to leave control over the Internet domain servers with the United States and instead called for an international forum to meet in future years to discuss Internet policy issues (Miller and Rhoads, 2005). For its part, the United States is currently loathe to give up control over the Internet as originally envisaged by earlier presidents.

Can the Internet Be Controlled?

Early Internet advocates argued that the Internet was different from all previous technologies. They contended that the Internet could not be controlled, given its inherent decentralized design, its ability to cross borders, and its underlying packet switching technology that made monitoring and controlling message content impossible. Many still believe this to be true today. The slogans are "Information wants to be free," and "the Net is everywhere" (but not in any central location). The implication of these slogans is that the content and behavior of e-commerce sites—indeed Internet sites of any kind—cannot be "controlled" in the same way as traditional media such as radio and television. However, attitudes have changed as many governments and corporations extend their control over the Internet and the World Wide Web (Markoff, 2005).

In fact, the Internet is technically very easily controlled, monitored, and regulated from central locations (such as network access points, as well as servers and routers throughout the network). For instance, in China, Saudi Arabia, North Korea, Thailand, Singapore, and many other countries, access to the Web is controlled from government-owned centralized routers that direct traffic across their borders and within the country, such as China's "Great Firewall of China," which permits the government to block access to certain U.S. or European Web sites, or via tightly regulated ISPs operating within the countries. In China, for instance, all ISPs need a license from the Ministry of Information Industry (MII), and are prohibited from disseminating any information that may harm the state or permit pornography, gambling, or the advocacy of cults. In addition, ISPs and search engines such as Google, Yahoo, and MSN typically self-censor their Asian content by using only government-approved news sources. MySpace also self-censors content it believes might upset the Chinese government. Despite this, in October 2007, it was reported that China was redirecting traffic from search engines operated by Google, Microsoft and Yahoo to Chinese-operated Baidu.com (Ho, 2007; Elgin and Einhorn, 2006).

In some instances, the firms have also cooperated with the Chinese government's pursuit of bloggers and journalists as a condition of its continuing business in China. For instance, Yahoo has been roundly denounced for helping the Chinese government convict and sentence a man to ten years in jail for posting information to a U.S. Web site.

In the United States, as we have seen in our discussion of intellectual property, e-commerce sites can be put out of business for violating existing laws, and ISPs can be forced to "take down" offending content, or stolen content. Government security agencies such as the FBI can obtain court orders to monitor ISP traffic and engage in widespread monitoring of millions of e-mail messages. Under the USA PATRIOT Act, passed after the World Trade Center attack on September 11, 2001, American intelligence authorities are permitted to tap into whatever Internet traffic they believe is relevant to the campaign against terrorism, in some circumstances without judicial review. And many American corporations are developing restrictions on their employees' at-work use of the Web to prevent gambling, shopping, and other activities not related to a business purpose.

In the United States, efforts to control media content on the Web have run up against equally powerful social and political values that protect freedom of expression, including several rulings by the Supreme Court which have struck down laws attempting to limit Web content in the United States. The U.S. Constitution's First Amendment says "Congress shall make no law ... abridging the freedom of speech, or of the press." As it turns out, the 200-year-old Bill of Rights has been a powerful brake on efforts to control 21st-century e-commerce content.

PUBLIC GOVERNMENT AND LAW

The reason we have governments is ostensibly to regulate and control activities within the borders of the nation. What happens in other nations, for the most part, we generally ignore, although clearly environmental and international trade issues require multinational cooperation. E-commerce and the Internet pose some unique problems to public government that center on the ability of the nation-state to govern activities within its borders. Nations have considerable powers to shape the Internet.

TAXATION

Few questions illustrate the complexity of governance and jurisdiction more potently than taxation of e-commerce sales. In both Europe and the United States, governments rely on sales taxes based on the type and value of goods sold. In Europe, these taxes are collected along the entire value chain, including the final sale to the consumer, and are called "value-added taxes" (VAT), whereas in the United States, taxes are collected on final sales to consumers and are called consumption taxes. In the United States, there are 50 states, 3,000 counties, and 12,000 municipalities, each with unique tax rates and policies. Cheese may be taxable in one state as a "snack food" but not taxable in another state (such as Wisconsin), where it is considered a basic food. Consumption taxes are generally recognized to be regressive because they disproportionately tax poorer people, for whom consumption is a larger part of total income.

Sales taxes were first implemented in the United States in the late 1930s as a Depression era method of raising money for localities. Ostensibly, the money was to be used to build infrastructure such as roads, schools, and utilities to support business development, but over the years the funds have been used for general government purposes of the states and localities. In most states, there is a state-based sales tax, and

a smaller local sales tax. The total sales tax ranges from zero in some states (North Dakota) to as much as 13% in New York City.

The development of "remote sales" such as mail order/telephone order (MOTO) retail in the United States in the 1970s broke the relationship between physical presence and commerce, complicating the plans of state and local tax authorities to tax all retail commerce. States sought to force MOTO retailers to collect sales taxes for them based on the address of the recipient, but Supreme Court decisions in 1967 and 1992 established that states had no authority to force MOTO retailers to collect state taxes unless the businesses had a "nexus" of operations (physical presence) in the state. Congress could, however, create legislation giving states this authority. But every congressional effort to tax catalog merchants has been beaten back by a torrent of opposition from catalog merchants and consumers, leaving intact an effective tax subsidy for MOTO merchants (Swisher, 2001).

The explosive growth of e-commerce, the latest type of "remote sales," has once again raised the issue of how—and if—to tax remote sales. Since its inception, e-commerce has benefited from a tax subsidy of up to 13% for goods shipped to high sales tax areas. Local retail merchants have complained bitterly about the e-commerce tax subsidy. E-commerce merchants have argued that this new form of commerce needs to be nurtured and encouraged in its early years, and that in any event, the crazy quilt of sales and use tax regimes would be difficult to administer for Internet merchants. State and local governments meanwhile see a potential source of new revenue slipping from their reach.

In 1998, Congress passed the Internet Tax Freedom Act, which placed a moratorium on "multiple or discriminatory taxes on electronic commerce" as well as on taxes on Internet access, for three years until October 2001, and in November 2001, extended the moratorium to November 2003. In November 2002, delegates from 32 states approved model legislation designed to create a system to tax Web sales. Spearheaded by the National Governor's Association (NGA), the Streamlined Sales Tax Project (SSTP) requires participating states to have only one tax rate for personal property or services effective by the end of 2005. By 2007, 15 states had agreed to support the SSTP. The governors are trying to get Congress to override judicial opinions and force online merchants to start collecting taxes. Nevertheless, in December 2004, Congress enacted the Internet Tax Nondiscrimination Act (Public Law 108–435), which extended the moratorium on states and local governments imposing taxes on Internet access and taxes on electronic commerce through November 1, 2007. In October 2007, Congress extended the moratorium once again, this time for an additional seven years. (Gross, 2007).

The merger of online e-commerce with offline commerce further complicates the taxation question. Currently, almost all of the top 100 online retailers collect taxes when orders ship to states where these firms have a physical presence. But others, like eBay, still refuse to collect and pay local taxes, arguing that the so-called tax simplification project ended up with taxes for each of 49,000 ZIP codes, hardly a simplification (Broache, 2005). The taxation situation is also very complex in services. For instance, none of the major online travel sites collect the full amount of state and local hotel occupancy taxes, or state and local airline taxes. Instead of remitting sales

tax on the full amount of the consumer's purchase, these sites instead collect taxes on the basis of the wholesale price they pay for the hotel rooms or tickets (Hansell, 2002).

The taxation situation in Europe, and trade between Europe and the United States, is similarly complex. The Organization for Economic Cooperation and Development (OECD), the economic policy coordinating body of European, American, and Japanese governments, is currently investigating different schemes for applying consumption and business profit taxes for e-commerce digitally downloaded goods. The EU began collecting a VAT on digital goods such as music and software delivered to consumers by foreign companies in 2003. Previously, European Union companies were required to collect the VAT on sales to EU customers, but U.S. companies were not. This gave American companies a huge tax edge.

Thus, there is no integrated rational approach to taxation of domestic or international e-commerce (Varian, 2001). In the United States, the national and international character of Internet sales is wreaking havoc on taxation schemes that were built in the 1930s and based on local commerce and local jurisdictions. Although there appears to be acquiescence among large Internet retailers such as Amazon to the idea of some kind of sales tax on e-commerce sales, their insistence on uniformity will probably delay taxation for many years, and any proposal to tax e-commerce will likely incur the wrath of almost 120 million U.S. e-commerce consumers. Congress is not likely to ignore their voices.

NET NEUTRALITY

In the United States, another Internet governance issue that has recently attracted attention has been the issue of "Net neutrality". Currently, all Internet traffic is treated equally (or "neutrally") by Internet backbone owners. However, telephone and cable companies that provide the Internet backbone would like to be able to charge differentiated prices based on the amount of bandwidth consumed by content being delivered over the Internet. The content of companies that pay an additional fee would be given preferential treatment in terms of delivery speed. The content of companies that refused to pay would be delivered at a slower rate. Those who oppose this prospect have been lobbying Congress to create a new layer of Internet regulation that would require network providers to manage their networks in a nondiscriminatory manner. So far, Congress has not yet passed any legislation, although the issue is likely to be revisited as certain types of content, such as online videos and other types of file-sharing, consume more and more bandwidth.

8.5 PUBLIC SAFETY AND WELFARE

Governments everywhere claim to pursue public safety, health, and welfare. This effort produces laws governing everything from weights and measures to national highways, to the content of radio and television programs. Electronic media of all kinds (telegraph, telephone, radio, and television) have historically been regulated by governments seeking to develop a rational commercial telecommunications environ-

In this chapter, we discuss social networks, auctions, and portals. One might ask, "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 thousands of 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, was formed in San Francisco in 1985 by a small group of people who once shared an 1800-acre commune in Tennessee. The Well is a online community that now has 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 Web 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 Web site hosting service based on neighborhoods. By 2002, however, the nature of online communities had begun to change. Cell phones and mobile Internet devices provided widespread access, making it possible to communicate nearly instantly with friends and relatives, and keep track of one another in a way not possible before. User-created Web sites called blogs became inexpensive and easy to set up without any technical expertise. These

technologies also enabled sharing of rich media such as photos and videos made possible by the spreading use of digital cameras, digital video cameras, cell phones with cameras, and portable digital music players. 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 networking was 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. The new social networking culture is very personal and "me" centered, displaying photos and broadcasting personal activities, interests, hobbies, and relationships on social network profiles. 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. About 60% of all Internet users in the United States—about 100 million Americans—have at one time or another gone online to a social network site (Pew Internet and American Life, 2007). MySpace reports storing 100 million profiles, and Facebook reports 39 million.

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 among members, and (d) people who share an area for some period of time (Hillery, 1955; Poplin, 1979). 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.

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

Now it's a short step to defining an **online social network** as an area online 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 DIFFERENCE BETWEEN SOCIAL NETWORKS AND PORTALS

We describe portals in the last section of this chapter. Portals began as search engines and then added content, Internet, and e-commerce services. In order to survive, portals have added many community-building and social networking features including chat groups, bulletin boards, free Web site design and hosting, and other

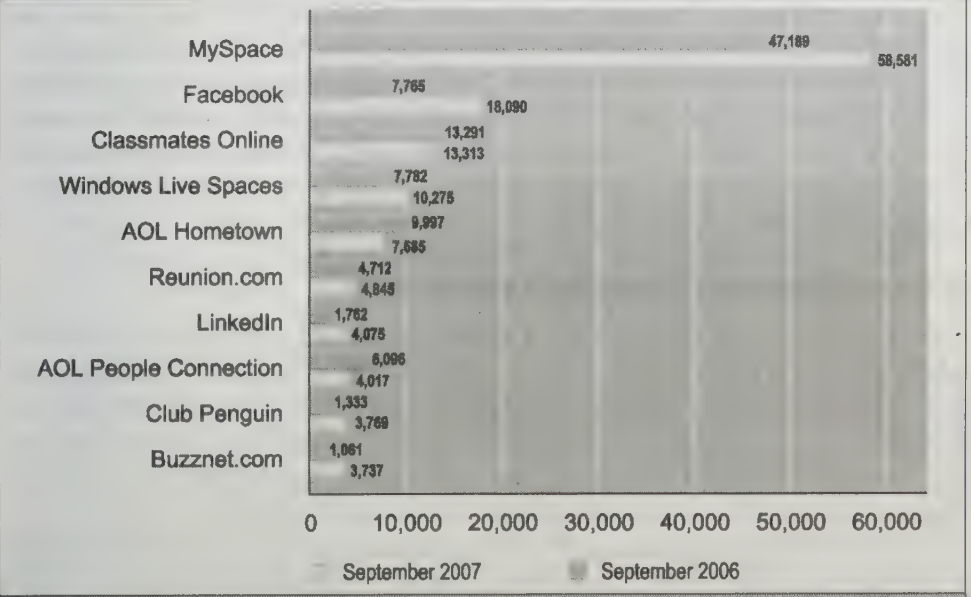
features that encourage visitors to stay on the site and interact with others who share their interests. Yahoo, for instance, uses deep vertical content features to retain its audience on site and maximize revenue opportunities. Portals have begun to measure their success in terms of their social networking features. For instance, Yahoo has purchased several Web properties, such as Flickr (a photo-sharing site) and HotJobs, which have social network features. Portals have moved toward becoming general community meeting places in an effort to enlarge and retain audience share and increase revenues. User-generated content on portals is one way to entice visitors to stay online at the site (and of course view more commercials).

Similarly, sites that began as narrowly focused content or affinity group community sites, such as iVillage, a site devoted to women's issues, have added more general portal-like services including general Web searching, general news, weather, travel information, and a wide variety of e-commerce services, often provided by portals seeking alliances. Browsers such as Mozilla's Firefox and Microsoft's Internet Explorer 7 are adding social networking features as well. There is no reason why social networking has to be limited to self-proclaimed social network sites such as MySpace. Social networking is a functionality, not a Web site. As a result, social networks and portals have moved closer together and at times are indistinguishable from one another.

THE GROWTH OF SOCIAL NETWORKS AND ONLINE COMMUNITIES

MySpace, Friendster, Tribe Networks, Flickr, and Facebook are all popular examples of online communities. **Figure 11.1** shows the top 10 social network sites, which together account for well over 90% of the Internet's social networking activity.

FIGURE 11.1 TOP 10 SOCIAL NETWORK SITES



SOURCE: Based on data from eMarketer, Inc., 2007a; Nielsen/NetRatings, 2007.

Sponsored communities are online communities created by government, nonprofit, or for-profit organizations for the purpose of pursuing organizational goals. These goals can be diverse, from increasing the information available to citizens; for instance, a local county government site such as Westchestergov.com, the Web site 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.

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

SOCIAL NETWORK FEATURES AND TECHNOLOGIES

Social networks have developed software applications that allow users to engage in a number of activities. Not all sites have the same features, but there is an emerging feature set among the larger communities. Some of these software tools are built into the site, while others can be added by users to their profile pages as widgets (described in earlier chapters). **Table 11.2** describes some of social network functionalities.

THE FUTURE OF SOCIAL NETWORKS

While today's social networking scene is highly concentrated among the top 10 general networking sites, this is unlikely to remain the case. Networks are springing up all over the Internet based on intensely felt interests of smaller groups of people,

TABLE 11.2 SOCIAL NETWORK FEATURES AND TECHNOLOGIES

FEATURE	DESCRIPTION
Profiles	Users can create Web pages that describe themselves on a variety of dimensions.
Friends network	Ability to create a linked group of friends.
Network discovery	Ability to find other networks and find new groups and friends
Favorites	Ability to communicate favorite sites, bookmarks, content, and destinations.
E-mail	Send e-mail within the social network sites to friends.
Storage	Storage space for network members, content.
Instant messaging	Immediate one-to-one contact with friends through the community facility.
Message boards	Posting of messages to groups of friends, and other groups' members.
Online polling	Polling of member opinion.
Chat	Online immediate group discussion; Internet relay chat (IRC)
Discussion groups	Discussion groups and forums organized by topic.
Experts online	Certified experts in selected areas respond to queries.
Membership management tools	Ability of site managers to edit content, and dialog; remove objectionable material; protect security and privacy.

draining potential members from the general sites. General networking sites are poor places to meet new people, and most online social networks reflect offline friendships and associations.

Today's networks are places you go online, but in the future, browsers, portals like Yahoo and Google, and general Web sites will have social networking functionality built in, making it less necessary that you go to a social network site, and more likely that social networking will come to you (see *Insight on Technology: Social Operating Systems: Facebook vs. Google*). The biggest Web e-mail services (who also happen to be the big portals) are adding features that allow users to perform sociable functions like tracking friends, creating profiles, and joining other groups. Yahoo's 250 million e-mail users globally together are arguably the world's largest inactive and undiscovered network. Network aggregators are also emerging: SocialURL, ProfileFly, and ProfileLinker allow people to aggregate feeds from their different social network profiles, making it less necessary to visit the destination site itself.

11.2 ONLINE AUCTIONS

Online auction sites are among the most popular consumer-to-consumer (C2C) e-commerce sites on the Internet. The market leader in C2C auctions is eBay, which has 222 million registered users (one of the largest registered customer bases on the Internet) from all over the world, 86 million active users in the United Stats, over 12 million items listed each day within 18,000 categories, and in 2006, $6 billion in net revenues, a 30% growth over the previous year (eBay Inc., 2007). 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 just about any good can be found for sale. Increasingly, established portals and online retail sites—from Yahoo and MSN to JCPenney and Sam's Club—are adding auctions to their sites. And, as noted in Chapter 12, auctions constituted a significant part of all B2B e-commerce in 2007, and over a third of procurement officers use auctions to procure goods. What explains the extraordinary popularity of auctions? Do consumers always get lower prices at auctions? Why do merchants auction their products if the prices they receive are so low?

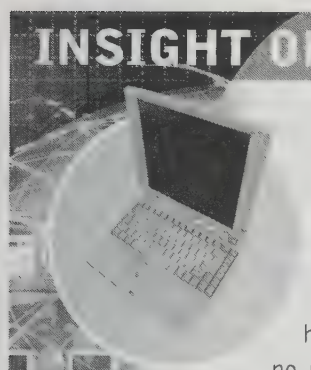
auctions
markets in which prices are variable and based on the competition among participants who are buying or selling products and services

dynamic pricing
the price of the product varies, depending directly on the demand characteristics of the customer and the supply situation of the seller

DEFINING AND MEASURING THE GROWTH OF AUCTIONS AND DYNAMIC PRICING

Auctions are markets in which prices are variable and based on the competition among participants who are buying or selling products and services. Auctions are one type of **dynamic pricing**, in which the price of the product varies, depending directly on the demand characteristics of the customer and the supply situation of the seller. There is a wide variety of dynamically priced markets, from simple haggling, bartering, and negotiating between one buyer and one seller, to much more sophisticated public auctions in which there may be thousands of sellers and thousands of buyers, as in a single stock market for a bundle of shares.

INSIGHT ON TECHNOLOGY



SOCIAL OPERATING SYSTEMS: FACEBOOK VS. GOOGLE

In the ongoing battles between hype and substance, fantasy and reality, hubris and humility, Silicon Valley takes no prisoners and has no equals. Google wants to organize the world's information, Amazon wants to be the world's store, and now Facebook wants to be the "social operating system" for the Internet, according to founder and CEO Mark Zuckerberg. Facebook wants to connect the world in one big social network (that it owns). Microsoft, owner of the world's desktops with a 95% market share, will just have to move on over while Facebook engineers this feat.

What can a social operating system possibly be? When we think of an operating system like Windows or Mac OS or Linux, we think of a software tool that controls the resources of the computer and provides the platform on which applications are built, launched, and operate. How can Facebook replace this? The answer is, it can't. But what Facebook can do is build, or encourage others to build, thousands of software applications, from tools such as iLike that let you find friends who share your musical tastes, to PopFly, a tool that lets you create links to Windows applications and Facebook, to the *Washington Post's* "political compass" application that allows you to calculate your place on a political spectrum of your friends, to games like Red Bull Roshambull, and a new program to "poke" people (mostly people of the opposite sex that you would like to know). iLike is now making more money on Facebook selling ads, and getting commissions from selling songs, and concert tickets, than it does from its own Web site, iLike.com.

In May 2007, Zuckerberg announced Facebook's new strategy of opening up its technology platform to outside developers or anyone who want to write an application and make it available to Facebook users. In short, Facebook is taking its two major assets—the 30 million unique users who visit each month, and its technology—and making them available to everyone. This allows developers to develop widgets and other Java applications to perform thousands of different tasks, and even allows developers to use their widgets to display ads and keep all the revenues. Facebook then becomes a kind of Web inside the Web—a platform or area where Web pages created by users (called "profiles") are linked together by the users themselves into networks, and where the applications are supplied by outside developers.

At some point in the future, these applications could include typical Office functionality like word processing and spreadsheets. But probably not, because these applications are already well performed by Microsoft Office and others. Instead businesses will be turning to Facebook to enhance the productivity of their employees by developing collaboration and meeting tools. Is Microsoft worried? Probably not, because people will still need a Windows or other operating system such as Mac OS to gain access to Facebook. So the social network operating system is not a substitute for a computer operating system. Not yet. Does Microsoft want to play in this new arena? Yes. It invested $250 million in Facebook in October 2007 for a 1.6% stake. This valued Facebook at $15 billion, and is a sign of how desperate Microsoft is to play in this new field. Facebook has revenue of only $200 million a year. It's quite a distance to $15 billion.

Not to be outdone by a mere start-up, Google refuses to give up the top spot in Silicon Valley's pantheon of creative genius. If Face-

(continued)

book promises to connect the world, Google wants to make sure it can play there too. Actually, Google wants to create a social networking world that runs on its standards and that would be universal to all social networks now and in the future. The problem with Facebook's opening to the world is that it's a closed world and creates applications that run only on Facebook. There are thousands of social networks that are more specialized, and are growing at faster rates than the big general social networks like Facebook and MySpace. Instead, Google has created a set of standard programs that enable three generic social network core functions and would be usable on all social networks. You can see these programs at Opensocial.com. These core functions are profile information (user data), friends information (social graph), and activities (events like news, schedules, reports of friends movements).

OpenSocial already has many friends who will host these applications: Engage, Friendster, hi5, Hyves, imeem, LinkedIn, MySpace, Ning, Oracle, Orkut, Plaxo, Salesforce.com, Six Apart, Tianji, Viadeo, and XING. Developers include Flixster, iLike, Friendster, Viadeo and Oracle, along with thousands of individual small developers. There seems to be a business network of social networking companies. The advantage for developers is that they can develop one application and have it run on all social networks. Another advantage is that this functionality can be added to any program, browser, or Microsoft Office application. For instance, you might be working on a particularly annoying spreadsheet and get help instantly from one of your business pals who's a wiz at spreadsheets. Or be in a Word document and suffer a loss of words. What better time to call in help from your friends? One consequence is that social networking functionality can be added to any program, and you will no longer have to go a social network site like Facebook in order to network. Social networking is a functionality, not a URL.

The company that seems to be in the crosshairs of all this activity is MySpace, the leading social network site by orders of magnitude. They have built a closed platform and do not allow outside developers to create applications, and certainly not to collect advertising revenues. It remains to be seen how long MySpace can maintain this isolation.

SOURCES: "Why So Many Want to Create Facebook Applications," by Riva Richmond, *Wall Street Journal*, September 4, 2007; "Facebook Gets Help From Its Friends," *Wall Street Journal*, June 22, 2007; "Exclusive. Facebook's New Face," by David Kirkpatrick, *Fortune*, May 25, 2007; "Facebook Opens Its Pages As a Way to Fuel Growth," *Wall Street Journal*, May 21, 2007.

In dynamic pricing, merchants change their prices based on both their understanding of how much value the customer attaches to the product and their own desire to make a sale. Likewise, customers change their offers to buy based on both their perceptions of the seller's desire to sell and their own need for the product. If you as a customer really want the product right now, you will be charged a higher price in a dynamic pricing regime, and you will willingly pay a higher price than if you placed less value on the product and were willing to wait several days to buy it. For instance, if you want to travel from New York to San Francisco to attend a last-minute business conference, and then return as soon as possible, you will be charged twice as much as a tourist who agrees to stay over the weekend.

In contrast, traditional mass-market merchants generally use **fixed pricing**—one national price, everywhere, for everyone. Fixed pricing first appeared in the nineteenth century with the development of mass national markets and retail stores that could sell to a national audience. Prior to this period, all pricing was dynamic and local, with prices derived through a process of negotiation between the customer and the merchant. Computers and the development of the Internet have contributed to a return of dynamic pricing. The difference is that with the Internet, dynamic pricing can be conducted globally, continuously, and at a very low cost.

fixed pricing
one national price, everywhere, for everyone

There are many other types of dynamic pricing that preceded the Internet. Airlines have used dynamic pricing since the early 1980s to change the price of airline tickets depending on available unused capacity and the willingness of business travelers to pay a premium for immediate bookings. Airline yield management software programs seek to ensure that a perishable item (an empty airline seat is useless once the plane takes off) is sold before flight time at some price above zero.

The use of coupons sent to selected customers, and even college scholarships given to selected students to encourage their enrollment, are a form of both price discrimination and dynamic pricing. In these examples, the price of the item is adjusted to demand and available supply, and certain consumers are discriminated against by charging them higher prices while others are advantaged by receiving lower prices for the same products, namely, a reduced price for an item or a college education.

trigger pricing
adjusts prices based on the location of the consumer

utilization pricing
adjusts prices based on utilization of the product

personalization pricing
adjusts prices based on the merchant's estimate of how much the customer truly values the product

Newer forms of dynamic pricing on the Internet include bundling, trigger pricing, utilization pricing, and personalization pricing. As discussed in Chapter 7, bundling of digital goods is the practice of including low-demand products in a bundle "for free" in order to increase total revenues. **Trigger pricing**, used in m-commerce applications, adjusts prices based on the location of the consumer—for example, walking within 400 yards of a restaurant may trigger an immediate 10% dinner coupon on a portable Web device. **Utilization pricing** adjusts prices based on utilization of the product; for example, Progressive Insurance Company adjusts the annual cost of automobile insurance based on mileage driven. **Personalization pricing** adjusts prices based on the merchant's estimate of how much the customer truly values the product; for instance, Web merchants may charge committed fans of a musician higher prices for the privilege of receiving a new DVD before its official release to retail stores. Higher-cost hardbound books sell primarily to committed fans of writers, while less-committed fans wait for cheaper paperback versions to appear. For a look at some of the controversial issues of dynamic pricing, read *Insight on Society: Dynamic Pricing: Is This Price Right?*

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
auction house sells goods it owns, or controls, using various dynamic pricing models

Auctions—one form of dynamic pricing mechanism—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. Less well known are **business-to-consumer (B2C)** auctions where a business owns or controls assets and uses dynamic pricing to

INSIGHT ON SOCIETY

DYNAMIC PRICING: IS THIS PRICE RIGHT?

How do you set the price for goods on the Internet? Following an ancient Phoenician formula, most retailers calculate costs and multiply by two to come up with a price. But, this was just the beginning of the pricing process. Ancient merchants then went to market where they had to haggle before getting the sale. For a wealthy looking prospect, the price might start out very high, and for a commoner, at a much lower price. This kind of dynamic pricing can be found in the earliest of marketplaces: adjusting the price to a variety of market factors, including general demand, product-specific demand, supply, and specific attributes of the customer.

Now there are a host of online and offline dynamic pricing tools that can calculate what prices the market will bear at any given moment, for any given personal situation of the consumer. With new Web-based tools, there's a perfect price for every time of day, every hour, and for every customer. Hold on to your wallets!

There are many different kinds of dynamic pricing. Time-based dynamic pricing adjusts the price to different points in the product life cycle, charging more in the beginning with a new product because many customers want the latest fashions, music, literature, computers, and other innovations. Peak-load dynamic pricing adjusts prices to times of the day when the supply is relatively fixed. Clearance dynamic pricing is used when products lose value over time. All types of dynamic pricing segment the market according to the willingness of customers to pay through different channels, at different times, and with different amounts of effort. Just about all economic models of dynamic pricing assume a nearly perfect rational consumer who will always and instantly react to price changes (so-called "unbounded rationality"). We all have friends who seem like this sometimes and are willing to chase a deal for even marginal gains.

Web-based dynamic systems developed by SAP, DemandTec Inc., Hewlett-Packard, and General Electric sift through massive databases crammed with up-to-date information on orders, promotions, product revenues, and stock levels in warehouses. Based on this information, a pricing plan is developed for nearly all products. On the Web, menu costs—the cost of adjusting prices—are very low, and pricing plans can be implemented across the country nearly instantaneously. In the future, for offline physical stores, the dynamic pricing industry has solutions also: radio frequency tagging of price stickers in stores and electronic shopping cart screens attached to every physical shopping cart. Gartner estimates that 50% of the Global 2000 retailers have adopted dynamic pricing as their dominant pricing model.

DHL Worldwide Express used to establish its prices the old-fashioned way—one product, one price, across the nation and the world. Unfortunately, DHL's prices were often higher than those of rivals FedEx and UPS. "We knew we had to bring prices down, but didn't know by how much," says Aman Adinew, DHL's director of pricing and revenue management. To find out how to price products, DHL purchased dynamic pricing software from Zilliant Inc. in Austin, Texas. The system loaded in various test prices for services, including the prices of competitors. Then the system offered Web and telephone customers seeking rate information a number of different prices. DH L learned how low it needed to go in prices but still make a profit. Now DHL turns 25% of callers and Web queries into customers, up from 17% before, revenue is up 13%, and gross margins have jumped 5.4%.

In a recent survey, Consumer Reports Webwatch surveyed dynamic pricing at popular Web destinations. At BarnesandNoble, a hardcover book priced at $20.80 on Wednesday suddenly popped to $26.00 on Friday. The price for a pair of shoes at the fashion site Zappos increased $3.95 in four days. And after making multiple different reservations on Expedia and

(continued)

Travelocity, the researchers found real-time quotes on the precise same vacations based on the Web browser used, and whether the browser had cookies based on previous use of these sites.

Dynamic pricing has its opponents, such as consumer groups and individual consumers who oppose the idea of being exploited based on their personal situations. A June 2005 study by the Annenberg Center at the University of Pennsylvania found that nearly two-thirds of those surveyed believed incorrectly that it was illegal for online retailers to charge different people different prices. Almost 90% strongly objected to the idea of online stores charging people different prices for the same products based on information collected about their shopping habits. While the consuming public takes a dim view of paying, say, $500 more for an airline seat than the person next to them, marketing professors think dynamic pricing is a natural part of healthy markets where price is used to adjust supply and demand, as long as price discrimination does not take place along ethnic or religious lines. But when used badly, especially when the consumer becomes aware of paying a discriminate price that is higher (rather than lower—everyone loves a deal), then the merchant can pay a hefty price.

For instance, in September 2000, Amazon found itself in the midst of a public relations nightmare when customers in online chat rooms discovered that they had been charged different prices for the same DVDs. Amazon founder Jeff Bezos denied that the incongruent prices resulted from gathering customer purchasing and behavioral data, and claimed instead that they were simply the result of random price testing to determine the correct price point for the products. Amazon was forced to apologize and issue refunds to approximately 7,000 customers. Today, Amazon claims that it absolutely does not use dynamic pricing despite rumors that Amazon will adjust the prices for goods based on what the consumer has already put in their shopping carts. Carts with "high value" items suggest a wealthy customer who would pay higher prices.

Although some consumers become irate when they are charged more for a product than others, other reports on dynamic pricing have concluded that customers are also willing to pay more for quality and superior service, whether perceived or real. For instance, most customers are willing to pay for overnight shipping at a high price. It appears that some forms of dynamic pricing are acceptable and others not. Research on dynamic pricing has found that consumers find discrimination is considered fair as long as all buyers have the possibility to achieve all price levels. For instance, consumers think it's fair that someone pays less for a bottle of soda when they walk to a vendor's stand to get the drink, and more to have the soda delivered to them by a vendor. Consumers also consider it fair to pay a little less for a book online (and wait a week to get it), and pay a little more at a bookstore to get it immediately. Consumers find dynamic pricing unfair when they believe they never stand a chance to get the low price, never knew about it, could not reasonably find out about it, and, as a result, feel duped or taken advantage of.

Unfortunately, dynamic pricing on the Web seems to work most commonly when the consumer does not have a clue it is occurring. When price transparency is reduced, price discrimination flourishes. Most people on the Web (if not everywhere) are not unboundedly rational. Instead they are boundedly rational because they do not have perfect information, often cannot respond to random or instant changes in price even on the Internet, and would have to expend something to get more information. While the Internet probably increases price transparency when compared to physical markets, there are still plenty of opportunities to exploit consumers' bounded rationality.

SOURCES: "Pay Your Money, Or You're Taking a Chance," Consumer Reports, consumerwebwatch.org, July 6, 2007; "Dynamic Pricing of Network Goods With Boundedly Rational Consumers," by Roy Radner and Arun Sundararajan, Working Paper CeDEER, June, 2006; "Dynamic Pricing in Name-Your-Own-Price Channels: Bidding Behavior, Seller Profit, and Price Acceptance," by Ill-Horn Hann, Oliver Hinz and Martin Spann, WISE (Workshop on Information Systems and Economics), 2006; "What Consumers and Retailer Should Know About Dynamic Pricing," Knowledge@Wharton, July 27, 2005, "Web Sites Change Prices Based on Customers' Habits, by Anita Ramasastry, CNN.com, June 24, 2005; "Dynamic Pricing in Retail Will Only Work if Customers Approve," by Gartner (Hung LeHong) June 7, 2005; "Can differential prices be fair?," by J. Cox, J. *Journal of Product and Brand Management*, 10 (5), Cox, J. (2001); "The use and perceived fairness of price-setting rules in the bulk electricity market," by P. Dickson; and R. Kalapurakal, *Journal of Economic Psychology*, 15 (3), (1994).

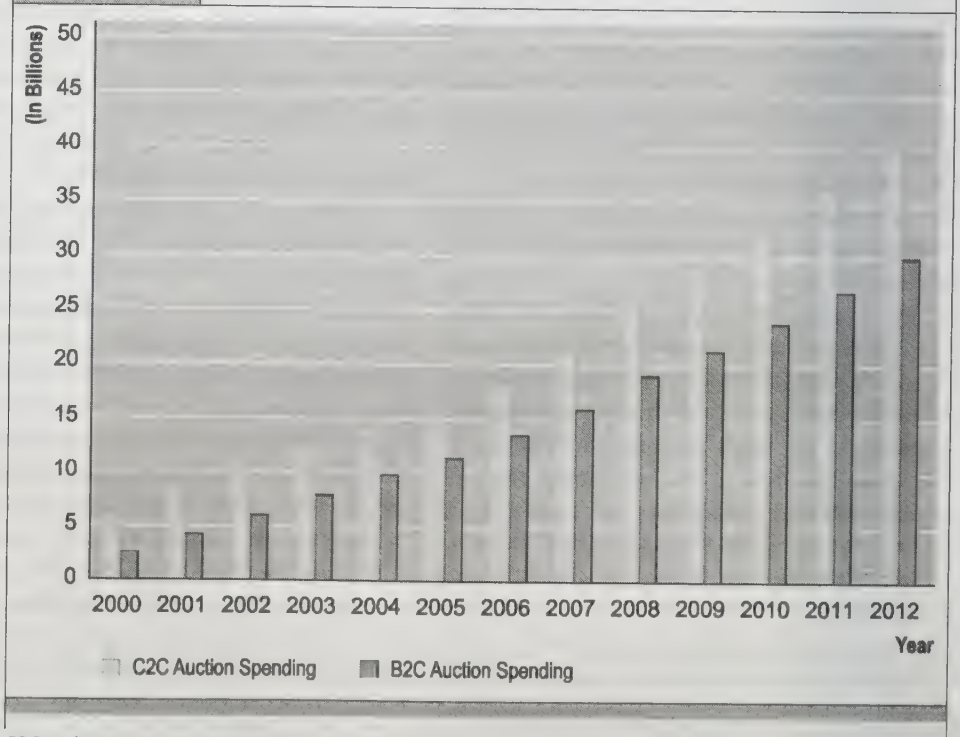
establish the price. Established merchants on occasion use B2C auctions to sell excess goods. This form of auction or dynamic pricing will grow along with C2C auctions. Online auctions are expected to grow in the range of 12%–18% annually between 2007 and 2012, with some firms such as eBay growing at 30% annually in large because of international expansion to new markets. In 2007, C2C auction sites in the United States generated about $21 billion in gross revenue, and B2C auction sites generated about $16 billion (see **Figure 11.3**).

Some leading online auction sites are listed in **Table 11.3**. 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).

WHY ARE AUCTIONS SO POPULAR? BENEFITS AND COSTS OF AUCTIONS

The Internet is primarily responsible for the resurgence in auctions. Although electronic network-based auctions such as AUCNET in Japan (an electronic automobile auction for

FIGURE 11.3 PROJECTED GROWTH IN AUCTION REVENUES



C2C and B2C auctions are expected to continue growing in the U.S. at double-digit rates through 2012.
SOURCES: Based on data from eMarketer, 2005; Jupiter Research, 2001; authors' estimates.

TABLE 21.3 LEADING ONLINE AUCTION SITES

GENERAL	
eBay	The world market leader in auctions: 66 million visitors a month and hundreds of thousands of products.
uBid	uBid has registered over 5 million customers and sold over $1 billion dollars in merchandise since it started in 1997. The company currently attracts over 2 million unique visitors a month.
BidZ	General merchandise. Over 2 million monthly visitors.
Auctions.amazon	General consumer and business close-out auctions. Over 1 million monthly visitors.
Bid4Assets	Liquidation of distressed assets from government and the public sector, corporations, restructurings, and bankruptcies. Over 200,000 visitors monthly.
Auctions.samsclub	Sam's Club brand merchandise in a variety of categories. Over 400,000 monthly visitors.
SPECIALIZED	
Racersauction	Specialized site for automobile racing parts.
Philatelicphantasies	Stamp site for professionals, monthly online stamp auction.
Teletrade	America's largest fully automated auction company of certified coins including ancient gold, silver, and copper coins. Also offers sports cards.
Baseball-cards.com	The Internet's first baseball card store. Offers weekly 5,000 plus lot auctions of baseball, football, basketball, hockey, wire photos, and more.
Oldandsold	Online auction service specializing in quality antiques. Dealers pay a 3% commission on merchandise sold.

used cars) were developed in the late 1980s, these pre-Internet auctions required an expensive telecommunications network to implement. 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 (Bapna, et al., 2001).

Benefits of Auctions

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

- **Liquidity:** Sellers can find willing buyers, and buyers can find sellers. The Internet enormously increased the liquidity of traditional auctions that usually required all participants to be present in a single room. Now, sellers and buyers can be located anywhere around the globe. Just as important, buyers and sellers can find a global market for rare items that would not have existed before the Internet.

- **Price discovery:** Buyers and sellers can quickly and efficiently develop prices for items that are difficult to assess, where the price depends on demand and supply, and where the product is rare. For instance, how could a merchant (or buyer) price a Greek oil lamp made in 550 B.C. (to use just one example of the rare items that can be found on eBay)? How could a consumer even find a Greek oil lamp without the Internet? It would be difficult and costly for all parties.
- **Price transparency:** Public Internet auctions allow everyone in the world to see the asking and bidding prices for items. It is difficult for merchants to engage in price discrimination (charging some customers more) when the items are available on auctions. However, because even huge auction sites such as eBay do not include all the world's online auction items (there are other auction sites in the world), there still may be more than one world price for a given item (there are inter-market price differences).
- **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. Online auctions provide consumers the chance to find real bargains at potentially give-away prices; they also provide access to a very wide selection of goods that would be impossible for consumers to physically access by visiting stores.
- **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. A sale at an auction can be consummated quickly and with very low transaction costs when compared to the physical world of markets.
- **Consumer aggregation:** Sellers benefit from large auction sites' ability to aggregate a large number of consumers who are motivated to purchase something in one marketspace. Auction-site search engines that lead consumers directly to the products they are seeking make it very likely that consumers who visit a specific auction really are interested and ready to buy at some price.
- **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. For instance, because eBay is so large—garnering close to 90% of all C2C auction commerce in the United States—it is quite likely you will find what you want to buy at a good price, and highly probable you will find a buyer for just about anything.

Risks and Costs of Auctions for Consumers and Businesses

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

- **Delayed consumption costs:** Internet auctions can go on for days, and shipping will take additional time. If you ordered from a mail-order catalog, you would likely

receive the product much faster, or if you went to a physical store, you would be able to obtain the product immediately.

- **Monitoring costs:** Participation in auctions requires your time to monitor bidding.
- **Equipment costs:** Internet auctions require you to purchase a computer system, pay for Internet access, and learn a complex operating system.
- **Trust risks:** Online auctions are the single largest source of Internet fraud. Using auctions increases the risk of experiencing a loss.
- **Fulfillment costs:** Typically, the buyer pays fulfillment costs of packing, shipping, and insurance, whereas at a physical store these costs are included in the retail price.

Auction sites such as eBay have taken a number of steps to reduce consumer participation costs and trust risk. For instance, auction sites attempt to solve the trust problem by providing a rating system in which previous customers rate sellers based on their overall experience with the merchant. Although helpful, this solution does not always work. Auction fraud is the leading source of e-commerce complaints to federal law enforcement officials. One 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. Also, most online auctions reduce monitoring costs by providing both a watch list and proxy bidding. **Watch lists** permit the consumer to monitor specific auctions of interest, requiring the consumer to pay close attention only in the last few minutes of bidding. **Proxy bidding** allows the consumer to enter a maximum price, and the auction software automatically bids for the goods up to that maximum price in small increments.

watch lists
permit the consumer to monitor specific auctions of interest

proxy bidding
allows the consumer to enter a maximum price, and the auction software automatically bids for the goods up to that maximum price in small increments

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. We explore the benefits and risks for merchants later in this chapter.

Market-Maker Benefits: 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. eBay has expanded into three lines of business that it believes are related: marketplaces (the original business), payments (PayPal), and communications (Skype). The strategy for eBay has been to make money off every stage in the auction cycle. eBay earns revenue 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. In addition, eBay purchased Skype, the Internet telephone company, so that buyers and sellers could communicate online with one another during the auction process. eBay has taken a significant write down in the value of Skype, but it remains the largest free Internet phone service.

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 BidZ and then Amazon 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

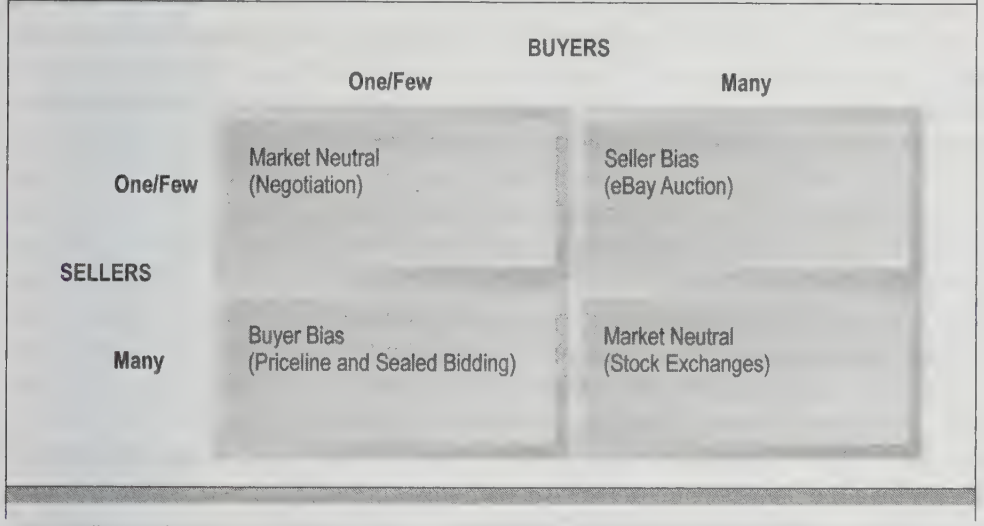
Auction theory is a well-established area of research, largely in economics (McAfee and McMillan, 1987; Milogram, 1989; Vickrey, 1961). Much of this research is theoretical, and prior to the emergence of public Internet auctions, there was not a great deal of empirical data on auctions or consumer behavior in auctions. Previous literature has identified a wide range of auction types, some of which are seller-biased, and others of which are more buyer-biased. Internet auctions are very different from traditional auctions (Morgan Stanley Dean Witter, 2000). Traditional auctions are relatively short-lived (such as a Sotheby's art auction), and have a fixed number of bidders, usually present in the same room. Online Internet auctions, in contrast, can go on much longer (a week), and have a variable number of bidders who come and go from the auction arena.

Internet Auction Basics

Before a business turns to auctions as a marketing channel, its managers need to understand some basic facts about online auctions.

Market Power and Bias in Dynamically Priced Markets Dynamically priced markets are not always "fair" in the sense of distributing market power to influence prices. **Figure 11.4** illustrates four different market bias situations that occur in dynamic markets.

FIGURE 11.4 BIAS IN DYNAMICALLY PRICED MARKETS



Dynamically priced markets can be either neutral or biased in favor of buyers or sellers.

In situations in which the number of buyers and sellers is few or equal in size, markets tend to be neutral, favoring neither the buyer nor the seller. One-on-one negotiations, barter markets, and stock exchanges all have this quality of neutrality, although specialists and market makers exact a commission for matching buy and sell orders. In stock markets, which are sometimes called a "double auction" because bids and offers are made continuously, many sellers and buyers call out prices for bundles of stock (of which there is a very large supply) until a deal is struck. In contrast, auctions such as those run by eBay and reverse auctions offered by companies such as Priceline have built-in biases. Usually on eBay, there is just one seller or a small number of sellers marketing goods that are in limited supply (or even rare goods) to millions of buyers who are competing on price. Priceline offers just the opposite bias and shares many features with a sealed-bid RFQ (request for quote) market. In Priceline's reverse auctions (described in greater detail later in this chapter), buyers post their unique needs for goods and services and a price they are willing to pay, while many sellers compete against one another for the available business. Of course, inherent bias in a marketplace does not mean consumers and merchants cannot find "good deals" and thousands of motivated customers willing to purchase goods at profitable prices.

However, the inherent biases should provide cautions to both merchants and consumers; namely, goods in auctions sometimes sell for far above their fair market value as they get bid too high, and sometimes for far less than their fair market value as merchants become too desperate for business. **Fair market value** could be defined here as the average of prices for that product or service in a variety of dynamic and fixed-price markets around the world. We explore other auction market failures in a later section.

fair market value
the average of prices for a product or service in a variety of dynamic and fixed-price markets around the world

uniform pricing rule
there are multiple winners and they all pay the same price

discriminatory pricing
winners pay different amounts depending on what they bid

Price Allocation Rules: Uniform vs. Discriminatory Pricing There are different rules for establishing the winning bids and prices in auctions where there are multiple units for sale, say, 10 IBM laptop PCs. With a **uniform pricing rule**, there are multiple winners and they all pay the same price (usually the lowest winning bid—sometimes called a market clearing price). Other auctions use **discriminatory pricing** in which winners pay different amounts depending on what they bid. See, for instance, Ubid.com, which typically auctions multiple units from manufacturers. Like so many other auction rules, price allocation can change bidding strategy in auctions. For instance, in a uniform pricing auction for 10 IBM laptops, you may bid a very high price for a few units, knowing that others will not follow, but you will only pay a price equal to the lowest winning bid needed to clear out the units from the market. The person who bid for the tenth unit may have only bid 75% as high as your offer. Nevertheless, that is the price you will actually pay—the price needed to "clear the market" of all units. However, under a discriminatory pricing rule, you would be forced to pay your high bid. Obviously, from a buyer's point of view, uniform pricing is better, but from a merchant's point of view, discriminatory pricing is much better.

bid rigging
bidders communicate prior to submitting their bids, and rig their bids to ensure that the lowest price is higher than it might otherwise be

price matching
sellers agree informally or formally to set floor prices on auction items below which they will not sell

Public vs. Private Information in Dynamically Priced Markets In some dynamic markets, the prices being bid are secret, and are known only to one party. For instance, a firm may issue a request for bid to electrical contractors for provision of electrical service on a new building. Bidders are requested to submit sealed bids, and the lowest bidder (subject to qualifications) will be the winner. In this instance, the bidders do not know what others are bidding, and must bid their "best" price. The danger here is **bid rigging**, in which bidders communicate prior to submitting their bids, and rig their bids to ensure that the lowest price is higher than it might otherwise be (which benefits the bidder, who in this instance is receiving the bid price as payment for services to be rendered). This is a common problem in sealed bid markets. However, in auction markets, bid prices are usually public information, available to all. Here the risks are that bidders agree offline to limit their bids, that sellers use shills to submit false bids, or that sellers use the market itself as a signaling device, driving prices up. Open markets permit large players to signal prices or engage in **price matching**, where sellers agree informally or formally to set floor prices on auction items below which they will not sell. Generally such collusion exists on the sell side, where there are just a few sellers or auction houses in a position to fix prices.

Types of Auctions

Now that you have learned some basic auction market rules and practices, it's time to consider some of the major forms of dynamically priced markets and auctions, both online and offline. **Table 11.4** describes the major types of auctions, how they work, and their biases. As you can see in Table 11.4, aside from the different formats and rules, there are many other differences among auctions. As noted above, there are both discriminatory and uniform pricing rules, although the latter seem to be most common. Also, in some auctions, there are multiple units for sale, whereas in others, there is only a single unit for sale. The major types of Internet auctions are English, Dutch-Internet, Name Your Own Price, and Group Buying.

TABLE 11.4 TYPES OF AUCTIONS AND DYNAMIC PRICING MECHANISMS

AUCTION TYPE	MECHANISM	BIAS
Sealed bid market (B2B e-procurement—Ariba Sourcing; eBay's Elance)	Sealed-bid auction, RFQs. Winner is chosen from lowest bidders at acceptable quality levels.	Buyer bias: Multiple vendors competing against one another.
Vickrey auction (private auction)	Sealed-bid auction, single unit; highest bidder wins at the second-highest bid price.	Seller bias: Single seller and multiple buyers competing against one another.
English auction (eBay)	Public ascending price, single unit; highest bidder wins at a price just above the second highest bid. Buyers can skip bidding at each price, but return at higher prices.	Seller bias: Single seller and multiple buyers competing against one another.
Dutch-traditional (Dutch flower market)	Public descending-price auction, single unit; seller lowers price until a buyer takes the product.	Seller bias: Single seller, and multiple buyers competing against one another.
Dutch-Internet (eBay Dutch Auction)	Public ascending price, multiple unit. Buyers bid on quantity and price. Final per-unit price is lowest successful bid, which sets a uniform price for all higher bidders as well (uniform price rule).	Seller bias: Small number of sellers and many buyers.
Japanese auction (private auction)	Public ascending price, single unit; highest bidder wins at a price just above second-highest bid (reservation price) and buyers must bid at each price to stay in auction.	Seller bias: Single seller and many buyers.
Yankee auction-Internet (variation on Dutch auction)	Public ascending price, multiple unit. Buyers bid on quantity and price per unit. Bidders ranked on price per unit, units, and time. Winners pay their actual bid prices (discriminatory rule).	Seller bias: Single seller and multiple buyers competing against one another.
Reverse auction	Public reverse English auction, descending prices, single unit. Sellers bid on price to provide products or services; winning bid is the lowest-price provider. Similar to sealed bid markets.	Buyer bias: Multiple sellers competing against one another.
Group buying (eSwarm)	Public reverse auction, descending prices, multiple units. Buyers bid on price per unit and units. Groups of sellers bid on price; winning bid is lowest-price provider.	Buyer bias: Multiple sellers competing against one another.
Name Your Own Price (Priceline)	Similar to a reverse auction except the price the consumer is willing to pay is fixed and the price offered is nonpublic. Requires a commitment to purchase at the first offered price.	Buyer bias: Multiple sellers competing against one another for an individual's business.
Double auction (NASDAQ and stock markets)	Public bid-ask negotiation; sellers ask, buyers bid. Sale consummated when participants agree on price and quantity.	Neutral: Multiple buyers and sellers competing against one another. Market bias: trading specialists (matchmakers)

NOTE: "Public" means all participants can observe prices offered.

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

English 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.

Traditional Dutch Auctions In the **traditional Dutch auction** in Aalsmeer, Holland, 5,000 flower growers—who own the auction facility—sell bundles of graded flowers to 2,000 buyers. The Dutch auction uses a clock visible to all that displays the starting price growers want for their flowers. Every few seconds, the clock ticks to a lower price. When buyers want to buy at the displayed price, they push a button to accept the lot of flowers at that price. If buyers fail to bid in a timely fashion, their competitors will win the flowers. The auction is very efficient: on average, Aalsmeer conducts 50,000 transactions daily for 15 million flowers. Dutch flower auctions are now conducted over the Internet. Buyers no longer have to be present at the market to bid, and sellers no longer have to have their flowers present in adjacent warehouses, but can ship directly from their farms (Kambil and vanHeck, 1996).

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

Dutch Internet Auctions In **Dutch Internet auctions**, such as those on eBay, OnSale, and others, the rules and action are different from the classical Dutch auction. 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 action is usually quite rapid, and proxy bidding is not used. **Table 11.5** shows closing data from a sample Dutch Internet auction for a bundle of laptop computers.

In Table 11.5, the bids are arranged by price and then quantity. Under a uniform pricing rule, the lowest winning bid that clears the market of all 10 laptops is $568 and all winners pay this amount. However, the lowest winning bidder, JB505, will only receive three laptops, not four, because higher bidders are given their full allotments.

Name Your Own Price Auctions Auctions pioneered by Priceline are the second most-popular auction format on the Web. Although Priceline also acts as an intermediary, buying blocks of airline tickets and vacation packages at a discount and selling them at a reduced retail price or matching its inventory to bidders, it is best known for its Name Your Own Price auctions, where 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 2007, Priceline had over 16 million registered users, 5.1 million visitors a month, and over $1 billion in revenues in 2007. It is the eighth-ranked travel site in

TABLE 11.5 A MULTI-UNIT DUTCH INTERNET AUCTION

CLOSING AUCTION DATA

Lot number	8740240
Total Number of Units	10
Description	HP Pavilion dv6500t Laptop; Win Vista; Intel Celeron 1.73 GHz, 1 MB L2 cache; 15" widescreen; 1 MB memory; Intel graphics accelerator
Reserve Price	None

BIDDER	DATE	TIME	BID	QUANTITY
JDMTKIS	11/25/07	18:35	$ 575	4
KTTX	11/25/07	18:55	$ 570	3
JB505	11/25/07	19:05	$ 568	4
VAMP	11/25/07	19:10	$ 565	2
DPVS	11/25/07	19:20	$ 565	1
RSF34	11/25/07	19:24	$560	1
CMCAL	11/25/07	19:25	$560	2

the United States. Today, it also arranges for the sale of new cars, hotel accommodations, car rentals, long distance telephone service, and home finance.

Table 11.6 describes the products and services available in Priceline's Name Your Own Price auctions. Clearly, a major attraction of Priceline is that it offers consumers a market biased in their favor and very low prices, up to 40% off. Brand-name suppliers compete with one another to supply services to consumers. However, it is unclear at this time if the Priceline business model can extend to other categories of products. Experiments to sell gasoline and groceries through Priceline failed.

But how can Priceline offer discounts up to 40% off prices for services provided by major name brand 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 consumer 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.

PRICELINE NAME YOUR OWN PRICE OFFERINGS

SERVICE/PRODUCT	DESCRIPTION
Airline seats	Brand-name carriers bid for individual consumer business—perishable items that airlines are motivated to sell at the last minute.
Hotel rooms	Brand-name hotels bid for consumer business—perishable services that hotels are motivated to sell on a last-minute basis.
Rental cars	Brand-name rental companies bid for consumer business—perishable services that rental companies are motivated to sell on a last-minute basis.
Vacation packages	Brand-name hotels and air carriers bid for consumer business—perishable services that providers are motivated to sell on a last-minute basis.
Cruises	Cruise ship companies bid for consumer business, especially active in off-season periods.

demand aggregators suppliers or market makers who group unrelated buyers into a single purchase in return for offering a lower purchase price. Prices on multiple units fall as the number of buyers increase

Group Buying Auctions: Demand Aggregators A **demand aggregator** facilitates group buying of products at dynamically adjusted discount prices based on high-volume purchases. The originator of demand aggregation was Mercata, formed in 1998, and the Web's largest retail demand aggregator until it ceased operations in January 2001, when needed venture capital financing did not materialize. Mercata holds several patents covering online demand aggregation. The largest supplier today of demand aggregation software is Ewinwin, a B2B demand aggregator. In general, demand aggregation did not work well for retail sales, but it has found a home in B2B commerce as a way of organizing group buying. Trade associations and industry-buying groups have traditionally pursued group buying plans in order to reduce costs from large suppliers.

Online demand aggregation is built on two principles. First, sellers are more likely to offer discounts to buyers purchasing in volume, and, second, buyers increase their purchases as prices fall. Prices are expected to dynamically adjust to the volume of the order and the motivations of the vendors.

Although online sites dedicated to retail group buying were not a commercial success, their software and business practices have been integrated into B2B and Business-to-Government (B2G) sites as one of many dynamic-pricing mechanisms. For instance, the federal government's Department of Homeland Security is building a centralized purchasing portal that will aggregate the demand for IT commodities (such as PCs, routers, and other equipment) from many different constituent agencies in order to reduce costs. In general, demand aggregation is suitable for MRO products (commodity-like products) that are frequently purchased by a large number of organizations in high volume.

Professional Service Auctions Perhaps one of the more interesting uses for auctions on the Web is eBay's marketplace for professional services, Elance. This auction is a sealed-bid, dynamic-priced market for freelance professional services from legal and marketing services to graphics design and programming. Firms looking for professional services post a project description and request for bid on Elance. Providers of services bid for the work. The buyer can choose from among bidders on the basis of both cost and perceived quality of the providers that can be gauged from the feedback of clients posted on the site. This type of auction is a reverse Vickrey-like auction where sealed bids are submitted and the winner is usually the low-cost provider of services. Another similar site is SoloGig.

Auction Aggregators (Mega Auctions) With thousands of auctions available on the Web, how can you, your customers, or your business find the right auction for products of interest that you want to either buy or sell? **Auction aggregators** (sometimes called mega auctions) offer one solution to this problem of multiple Internet markets and inter-market price differences. Auction aggregators use computer programs to search thousands of Web auction sites, accumulating information on products, bids, auction duration, and bid increments. Consumers search auction aggregator sites for products of interest, and the site returns a list of both fixed-price sales locations and auction locations where the product is for sale. Auction aggregators work by sending Web crawlers to thousands of auction sites every night (and on some sites during the day as well), gathering all information on product listings—just like an ordinary single consumer would. However, the major sites have effectively prevented auction aggregators from searching their sites without a license.

auction aggregators use computer programs to search thousands of Web auction sites, and aggregate information on products, bids, auction duration, and bid increments

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. Switch perspectives now to that of a business. Remember the objective for 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 11.7** provides an overview of factors to consider.

The factors to consider include:

- **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 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).