38

e-Business & e-Commerce

Objectives

- To understand how the Internet and World Wide Web are revolutionizing business processes.
- To introduce various business models used on the Web.
- To explore the advantages and disadvantages of creating an online business.
- To examine marketing, payment, security and legal issues that affect e-businesses.

O Gold! I still prefer thee unto paper, Which makes bank credit look like a bark of vapour!
Lord Byron

It is an immutable law in business that words are words, explanations are explanations, promises are promises—but only performance is reality.
Harold S. Green

My name is Sherlock Holmes. It is my business to know what other people don't know.
Sir Arthur Conan Doyle

When you stop talking, you've lost your customer.
Estee Lauder

Outline

Outline (Cont.)

38.1 Introduction

We are in the **Age of Knowledge**. The phrases "knowledge is power" and "content is king" are often used in reference to business conducted on the Internet. In the rather short history of e-business and e-commerce, events have demonstrated that successful e-businesses are those that recognize the needs of their target audiences and match them with relevant content. However, the ability to construct such an e-business is not limited to seasoned professionals—many successful online ventures have been started by students on college campuses.

The terms e-business and e-commerce, often used interchangeably, in fact have different meanings. According to Andrew Bartels, vice president and research leader of e-commerce trends at Giga Information Group, Inc., **e-commerce** refers to aspects of online business involving exchanges among customers, business partners and vendors. For example, suppliers interact with manufacturers, customers interact with sales representatives and shipment providers interact with distributors. **E-business** encompasses these elements, but also includes operations that are handled within the business itself. For example, production, development, corporate infrastructure and product management are aspects of e-business not included under the category of e-commerce.[1]

E-business and e-commerce have increased the speed and ease with which business can be transacted, resulting in intense competition among online vendors. To remain viable, e-businesses must adjust to evolving technologies, continually integrate new systems and satisfy a wide variety of consumers. If a business fails to do so, its customers do not have far to go to buy from competitors.

Currently, the online medium enables people to pay bills, write and cash checks, trade stocks, take out loans, mortgage their homes and manage assets from the comfort of their homes or offices. Money as we now know it has begun to be augmented by such technologies as smart cards and digital cash. Intelligent programs handle the financial and logistical aspects of interactions between individuals and corporations on the Internet. People need only a connection, a computer or handheld wireless device and a digital form of payment to shop online. (Online monetary transactions are discussed in Section 38.5.)

The construction and maintenance of an e-business, especially one that processes a large number of transactions, requires technical, marketing and advertising expertise. Customers want access to products and services on a **24/7** basis (24 hours per day, 7 days per week). They also expect reliable, functional, fast and user-friendly services; companies that provide such services have higher success rates. One option for the improvement of e-business processes is **personalization**, which facilitates efficient online shopping and the smooth conducting of e-business transactions. Personalization is achieved by tracking a consumer's movement through the Internet, combining this data with personal information provided by the consumer and employing the compiled information to customize interactions with Web sites and applications. (Personalization, marketing and customer relationship management are discussed in Section 38.4.)

Although personalization can increase the convenience of Internet navigation, some people consider it to be an invasion of privacy. Similar Internet privacy concerns arise regarding the sale of personal data collected by online organizations. Such information can include customers' names, addresses, purchasing history, credit-card numbers and medical history. We explore Internet privacy and legal issues in Section 38.7.

Another issue of concern is Internet security. As more and more transactions occur online and the volume of information transmitted over the Web continues to grow, it becomes harder to guarantee the confidentiality of this information. Consumers and business alike continue to search for ways to conduct secure and safe e-business. We introduce various Internet and wireless Internet security principles and solutions in Section 38.6.

The conversion of **brick-and-mortar** businesses (businesses that have only a physical presence) into **click-and-mortar** businesses (businesses that have both an online and an offline presence) has occurred worldwide in nearly every industry. Click and mortar businesses realize that an online presence teamed with a physical store presence could provide beneficial results (e.g., `Amazon.com`® teamed with Target stores—`Amazon.com` gains a physical/offline presence and Target builds its online presence). Businesses can now operate effectively without offices, because employees can communicate via phone, voice mail, fax, e-mail and the capabilities of the Internet and wireless Internet (wireless technology and mobile business are discussed in detail in Sections 38.9–38.14).

e-Fact 38.1

B2B E-Commerce revenues worldwide are expected to reach $2,367 billion by 2004.[2]

38.2 e-Business Models

The transition of a business into an e-business provides many benefits. An e-business can offer personalization, effective customer service and streamlined **supply-chain management** (the strategic management of distribution channels and the processes that support

them). In this section, we explore the different types of businesses operating on the Internet, and introduce the technologies needed to build and run an e-commerce Web site.

Although the term "e-commerce" is relatively new (it was coined in the early 1990s), large corporations have been conducting de facto e-commerce for decades by networking their computing systems with those of business partners and clients. For example, the banking industry uses **Electronic Funds Transfer (EFT)** to transfer money between accounts. In addition, many companies employ **Electronic Data Interchange (EDI),** which facilitates the standardization of such business forms as purchase orders and invoices, allowing companies to share information with customers, vendors and business partners electronically. Many companies are using XML to enhance or improve EDI as well (XML is discussed later in this chapter and in Chapter 20). Until recently, e-commerce was feasible only for large companies. However, by using the Internet and the Web, even the smallest businesses can use EDI.

`Amazon.com`®, eBay®, Yahoo!® and other e-commerce sites have assisted in defining industry categories and business models on the Web. Entrepreneurs starting e-businesses and people interested in e-commerce should be aware of the various e-business models currently in use. In the subsections that follow, we review the storefront model, the auction model, dynamic pricing models, the portal model and other Web business models.

38.2.1 Storefront Model

The **storefront model** is what many people think of when they hear the word "e-business." By providing a combination of transaction processing, security, online payment and information storage, the storefront model enables merchants to sell their products online. This model is a basic form of e-commerce in which buyers and sellers interact directly.

To conduct storefront e-commerce, merchants must organize online product catalogs, take orders through their Web sites, accept payments securely, send merchandise to customers and manage customer data (such as customer profiles). They must also market their sites to potential customers through various media. Examples include `www.gap.com`, `www.restaurant.com`, `www.walmart.com`, `www.barnesandnoble.com` and more.

38.2.2 Shopping-Cart Technology

One of the most commonly used e-commerce enablers is the **shopping cart**. This order-processing technology allows customers to accumulate items they wish to buy as they browse an e-business Web site. (See the `Amazon.com` feature.) Support for the shopping cart is provided by a product catalog, which resides on the **merchant server** in the form of a **database**. The merchant server is the data storage and management system employed by the merchant. Often, a network of computers performs all the functions necessary to run a Web site. A database is a section of the merchant server designed to store and report on large amounts of information. For example, a database for an online clothing retailer would typically include such product specifications as item description, size, availability, shipping information, stock level and on-order information. Databases also store customer information, including names, addresses, credit-card data and past purchases. The `Amazon.com` feature contains further information regarding these technologies and their implementations. Most Web sites that conduct e-business over the Internet today use shopping-cart technology, including `www.eddiebauer.com`®, `www.kbtoys.com`, `www.niketown.com`, `www.sears.com` and `www.jcrew.com`.

Amazon.com

One of the most widely recognized examples of an e-business that uses shopping-cart technology is Amazon.com.[3] Founded in 1994, the company has grown to become one of the world's largest online retailers. Amazon.com offers millions of products to customers in over 160 countries.[4] The site also hosts online auctions. Although Amazon.com originally served as a mail-order book retailer, its product line has expanded to include music, videos, DVDs, electronic cards, consumer electronics, hardware, tools, beauty items and toys. Amazon.com's catalog is growing constantly, not only as it adds new products, but as it partners with or buys additional company Web sites (such as ToysRUs and BabiesRUs). The site also facilitates convenient navigation among millions of products.

Amazon.com uses a database on the **server side** (the merchant's computer systems) that offers customers on the **client side** (the customer's computer or handheld device) multiple ways to search for products. This system exemplifies a **client/server application**. The Amazon.com database consists of product specifications, availability, shipping information, prices, sales histories, reviews and in-depth product descriptions. In addition to providing customers with details on items for sale, this extensive database enables Amazon.com to cross-reference products. For example, a novel can be listed under various categories, including **fiction**, **bestsellers** and **recommended titles**.

Amazon.com provides personalized service to returning customers. A database keeps records of users' previous transactions, including items purchased, shipping addresses and credit-card information. Upon returning to the site, customers are greeted by name and presented with lists of titles that are recommended to them on the basis of their previous purchases. This enables the company to offer personalization that would otherwise be handled by sales representatives. Amazon.com also uses customer data for data mining (i.e., searching for patterns and trends among its clientele). Such analysis of consumer behavior can help the company to improve its products and services.

The purchase process at Amazon.com is simple. The company's home page provides various search features and categorical options, allowing users to select the product or type of product they wish to locate. For example, the book *Internet & World Wide Web How to Program*, *Third Edition*, can be found by using the **Search** box on the home page. To purchase an item once it is found, users simply click the **Add to Shopping Cart** button on the page containing the item's details. The shopping-cart technology processes the information and displays a list of the products in the shopping cart (users can view their cart at any time while shopping by clicking **View Cart** at the top of the Web page). Users then can change the quantity of each item, remove an item from the shopping cart, check out or continue shopping.

When users are ready to place their orders, they proceed to checkout. First-time visitors are prompted to fill out a personal-identification form in which they provide their names, billing addresses, shipping addresses, shipping preferences and credit-card information. Users are also asked to enter a password that they will use to access account data during future transactions. Once the shipping, billing and password information is confirmed, orders can be placed.

Amazon.com (Cont.)

Customers returning to `Amazon.com` can use its **1-Click℠ system**. This patented system allows consumers to reuse previously entered payment and shipping information, enabling them to place orders with a single click of the mouse. The 1-Click system exemplifies how an intelligently designed database application can improve the efficiency and convenience of business transactions.[5]

When the order process is complete, `Amazon.com` sends a confirmation e-mail to the user. A second e-mail is sent when an order is shipped, and a database monitors the status of all shipments. Users can track the status of their purchases until they leave the `Amazon.com` shipping center by selecting the **Your Account** link at the bottom of the page and entering their passwords. This will bring them to an **Account Maintenance** page. Orders can be cancelled at any time before the product is shipped, which usually occurs within 24 to 48 hours of purchase. `Amazon.com` has regional warehouses from which it can ship most packages overnight without having to use express delivery services.

`Amazon.com` operates on secure servers that protect personal information. Users who feel uncomfortable about using their credit cards on the Web can initiate orders through Amazon's Web site by entering the last five digits of their credit-card numbers. To complete such orders, users call Amazon's Customer Service Department and provide the remaining numbers.

38.2.3 Auction Model

The Web offers a wide variety of auction sites, as well as sites that search auction sites to pinpoint the lowest prices on available items. Usually, auction sites act as forums through which Internet users can assume the role of either **seller** or **bidder**. Sellers can post items they wish to sell, the minimum prices they require to sell the items and deadlines to close the auctions. Some sites allow users to provide additional information, such as a photograph or a description of an item's condition. Bidders may search the site for items they are seeking, view the current bidding activity and place bids—usually in designated increments. Some sites automate the bidding process by allowing bidders to submit the maximum prices they will pay for auction items. On such sites, an electronic system continues bidding for a bidder until the bidder wins the auction or the auction surpasses the bidder's maximum bid price. One of the most popular auction sites on the Web today is eBay (`www.ebay.com`). (Auction technology is explained in more depth in the eBay feature.)

The **reverse-auction model** allows buyers to set prices that sellers compete to match, or even beat. One example of a reverse-auction site is `priceline.com`, which is a popular site for purchasing airline tickets and making travel reservations. Usually, Priceline can process buyers' bids within one hour. A faster bidding option is available to sellers who are willing to set **reserve prices.** Although a reserve price is the lowest price that a seller will accept, the seller can set a reserve price that is higher than the minimum bid. If no bids meet the reserve price, the auction is unsuccessful. Most sellers who set reserve prices at `priceline.com` receive a series of bids within one hour of their initial posting. However, successful bids on items with reserve prices are binding, meaning that the buyer and seller must commit.

Auction sites usually receive a commission on each sale. When an auction is complete, the seller and the winning bidder are notified, and they decide on methods of payment and delivery. Most auction sites do not usually involve themselves in payment or delivery, though eBay purchased PayPal to handle its electronic payments (see the PayPal feature in Section 38.5.2).

The auction model is also employed by **business-to-business (B2B)** Web sites. The buyers and the sellers in these auctions are companies. Companies use online auctions to sell excess inventory and to access new, price-sensitive customers. Three examples of B2B auction sites are `www.ubid.com`, DoveBid, Inc. (`www.dovebid.com`) and WorldCall Exchange (`www.worldcallexchange.com`).

eBay® and the Online Auction Model

Online auctions are a successful method of conducting e-commerce. eBay (`www.ebay.com`) is both the leading online auction Web site and one of the world's most profitable e-businesses (Fig. 38.1).[6] The online auction house's roots lie in a 50-year-old novelty item—Pez® candy dispensers. Pam Omidyar, an avid collector of Pez dispensers, came up with the idea of trading them over the Internet. In 1995, she and her husband created a company called AuctionWeb. The company, which was renamed eBay, now has as many as 16 million items available for auction across 27,000 categories, including antiques, cars, clothing, electronics, jewelry, real estate, toys, travel and more. [7]

People can buy and sell just about anything on eBay. The company collects both a submission fee and a percentage of each sale amount. Submission fees are based on the amount of exposure sellers want their items to receive. For example, an additional fee wins an item a place among the "featured auctions" in a specific product category, whereas an even higher fee is required to be listed on the eBay home page under **Featured Items**. Listings are shown on the home page periodically. Alternatively, sellers can publish their product listings in a boldface font (for an additional charge).

eBay uses a database to manage its auctions. This database evolves dynamically as sellers and buyers enter personal identification and product information. The seller entering a product to be auctioned provides a description of the product, keywords, an initial price, a closing date for the auction and personal information. eBay then uses this data to produce the product profile seen by potential buyers (Fig. 38.2).

The auction process begins when the seller posts a description of the item for sale and fills in the appropriate registration information. The seller must specify a minimum opening bid. If potential buyers think this price is too high, the item might not receive any bids. In many cases, a reserve price is also set. Sellers often set an opening bid that is lower than the reserve price to generate bidding activity.

If a successful bid is made, the seller and the buyer negotiate the shipping details, warranty and other particulars. eBay serves as a liaison between the parties, providing an interface through which sellers and buyers can conduct business. However, eBay does not maintain a costly physical inventory or deal with shipping, handling or other services that other e-retailers must provide.

eBay® and the Online Auction Model (Cont.)

Fig. 38.1 eBay home page. (These materials have been reproduced with the permission of eBay Inc. COPYRIGHT © EBAY INC. ALL RIGHTS RESERVED.)

eBay's success has had a profound effect on the e-business industry. The company's founders took a limited-access offline business model and, by using the Internet, were able to bring it to the desktops of consumers worldwide. By implementing traditional marketing strategies and keeping the process simple, eBay has created a viable alternative to storefront-style e-commerce. It has also had a network effect for online sellers and buyers. Sellers want to be where the buyers are and vice versa. Due to the fact that eBay was one of the first sites to offer this business model, its has grown not only in size but its established reputation continues to attract consumers and sellers as well.

Other online auction sites include Yahoo! Auctions (`auctions.yahoo.com`), Amazon Auctions (`www.amazon.com`), FairMarket, Inc. (`www.fairmarket.com`) and Sotheby's (`www.sothebys.com`).

eBay® and the Online Auction Model (Cont.)

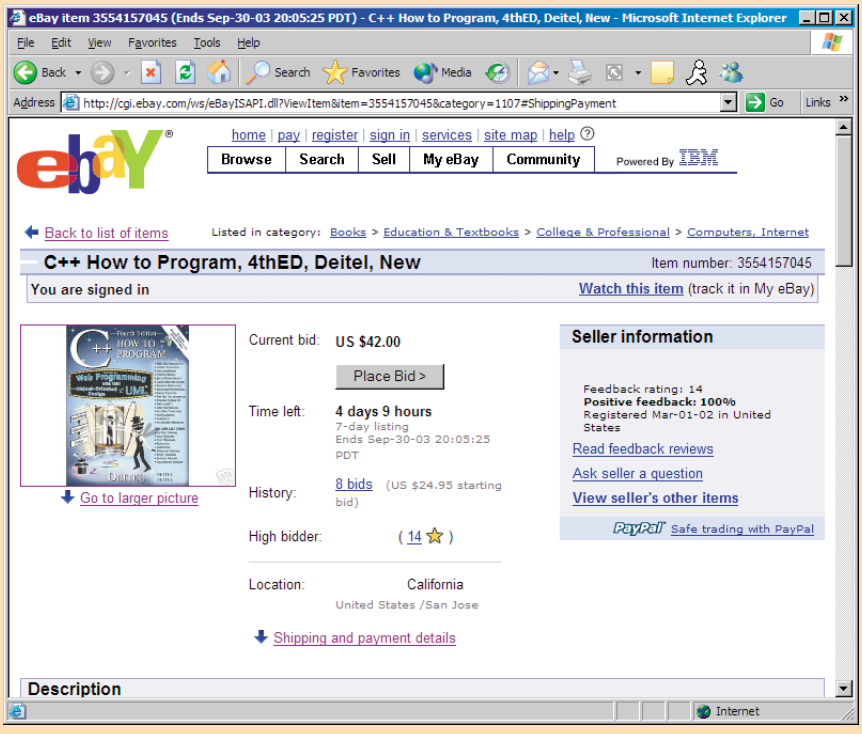

Fig. 38.2 Placing a bid on eBay. (These materials have been reproduced with the permission of eBay Inc. COPYRIGHT © EBAY INC. ALL RIGHTS RESERVED.)

38.2.4 Portal Model

Portal sites offer visitors the chance to find almost anything they are looking for in one place. They often provide news, sports and weather information, as well as the ability to search the Web. When most people hear the word "portal," they think of search engines. **Search engines** are **horizontal portals**, or portals that aggregate information on a broad range of topics. Other portals are more specific, offering a great deal of information pertaining to a single area of interest; such portals are called **vertical portals**.

Online shopping is a popular feature of many major portals. Sites such as `About.com`®, `altavista.com` and `Yahoo.com`® provide shopping pages that link users to thousands of sites carrying a variety of products.

Portals that link consumers to online merchants, online shopping malls and auction sites provide several advantages. These portals help users collect information on products and services, thus facilitating comparison shopping. Portals also allow users to browse

independently owned storefronts—a capability that some online shopping malls fail to provide. For example, Yahoo! permits users to browse a variety of sites while maintaining the convenience of paying through their Yahoo! account.

38.2.5 Name-Your-Price Model

The **name-your-price** business model empowers customers by allowing them to state the price they are willing to pay for products and services. Many e-businesses that offer this service have formed partnerships with leaders of various industries, such as travel, lending and retail. The online business passes each customer's price request to an appropriate industry partner, who decides whether to sell the product or service to the customer at the stated price. A customer whose price is rejected can offer another price. However, if a price is accepted, the customer is obligated to make the purchase. For example, `Priceline.com` allows users to submit prices they are willing to pay for airline tickets. However, before the request is submitted, users must enter their purchasing information, so that if their price is accepted by one of `Priceline.com`'s affiliate airlines, the user is required to purchase the ticket. On average, the user receives an e-mail response within one hour indicating whether the request is accepted or denied. If no affiliates are willing to offer an airline ticket to a user's destination for the specified price, the user can change the price and resubmit the bid.

Many e-businesses use **intelligent agents** (e.g., **shopping bots**) to enhance their Web sites. Intelligent agents are programs that search, arrange and analyze large amounts of data. Shopping bots can scour data contained within a single database or search the entire Web to find products and prices.

38.2.6 Comparison-Pricing Model

The **comparison-pricing model** allows customers to poll various merchants in search of the lowest price for a desired product or service. Comparison-pricing sites often generate revenue from partnerships with merchants. For example, `Travelocity.com` allows users to search multiple carriers and merchants for the best prices on airfares, hotels, rental cars, and other products. Other examples of Web sites that offer these services include `www.shopping.com`, `www.pricewatch.com` and `www.froogle.com` (see the Froogle feature). Although such sites can be convenient, users should be careful when employing these services, because they might not be getting the best prices available on the Web. Some services promote the products of merchants with which they have partnerships.

Froogle

People use the Internet as a preferred medium to purchase products and services. Whether it is buying a new car, a house, a pair of shoes, theater tickets, antiques or something else, users can find almost any for-sale product available on the Web. For example, in the third quarter of 2002 alone, consumers spent over $11 billion on the Internet.[8]

Froogle (Cont.)

As e-retailing continues to grow, Internet users want resources to help them seek out the best deal for their money. Froogle (`www.froogle.com`—developed by the same engineers who created the popular search engine Google) is a new service that uses search-engine technology to locate and rank information on for-sale items available worldwide. Launched in beta form in December 2002, it enables users to search for almost any product or type of product, compare prices and sort the results based on price (highest price to lowest price, or vice versa) or by stores that carry the product. The same principles used in searching for information on the Internet apply to these comparison-price search sites. Users can perform advanced searches that require more specific details about a product or service, or they can search a general category of products until they find a product of interest to them.[9]

Many view this technology as a new tool to enhance the consumer's shopping experience on the Web and allow consumers to be more informed about the products and services they wish to purchase. However, most of these sites are used for information only and provide users with the resource they need to find retailers that actually sell the product. For example, Froogle does not participate in the direct selling or buying of any product on which it provides information.

38.2.7 Bartering Model

Another popular e-business model is **bartering**, or the offering of one item in exchange for another. `ITEX.com` (formerly `Ubarter.com`™) allows individuals and companies to trade products through its site. At the site, traders make initial offers with the intention of bartering until they reach final agreements with buyers.

To conduct most transactions using this business model on the Web, potential customers send their pricing preferences to the merchant, who evaluates the offers. Final agreements often involve a combination of bartering and monetary payment.

38.3 Building an e-Business

There are numerous ways to design, develop and maintain an e-business. Some businesses establish online presences using **turnkey solutions**. (See the Yahoo! Small Business Merchant Solutions feature.) A turnkey solution is a prepackaged e-business. Another option for e-business development is an e-business template, which outlines the basic structure of the business, but allow the design to be determined by the owner. Alternatively, larger corporations and businesses with substantial funding can outsource the project to an organization that offers e-business solution packages. Large corporations also can build e-business solutions in-house.

38.4 e-Marketing

Competition is intense in the e-business and e-commerce worlds, and a solid e-marketing strategy can give a company an advantage. In this section, we explore various components of a **marketing campaign**, such as marketing research, advertising, promotions, branding

Yahoo! Small Business Merchant Solutions

Online **store-builder** solutions allow merchants to set up online storefronts, complete with catalogs, shopping carts and order-processing capabilities. Although these usually fixed-priced options are available to businesses of all sizes, they are ideal for small businesses that cannot afford custom solutions or do not possess secure merchant servers. *Yahoo! Small Business Merchant Solutions* is an e-commerce store-builder solution available at `smallbusiness.yahoo.com/merchant`.[10]

Yahoo! Small Business Merchant Solutions charges monthly fees on the basis of the number of items that users want to sell. Designed to simplify the process of creating an online store, this turnkey solution contains all the features necessary to build a complete e-commerce site.

To set up a working storefront where orders can be accepted, a user must sign on with Yahoo! Small Business Merchant Solutions and set up merchant accounts with banks, enabling the acceptance of credit-card payments. Generally, merchant banks and credit-card companies retain a small percentage of each transaction as their fee. (Online payments are discussed in Section 38.5.)

Yahoo! Small Business Merchant Solutions e-commerce sites are hosted on Yahoo! secure servers, which are maintained on a 24/7 basis. The site also backs up all the information needed to run a store and provides SSL technology to encrypt credit-card transactions. (We discuss SSL security in Section 38.6.5.)

Yahoo! Small Business Merchant Solutions merchants can track sales, analyze customers' paths through the Web to their sites and use the Yahoo! wallet. (E-wallets are discussed in Section 38.5.2.) In addition, Yahoo! lists each store in Yahoo! Shopping, allowing customers to access the store through a link at the Yahoo! Web site.[11]

and public relations (PR). We also discuss the importance of search engines and how they can be used to increase Web-site traffic.

38.4.1 Branding

A **brand** is typically defined as a name, logo or symbol that identifies a company's products or services. Brands should be unique, recognizable and easy to remember. **Brand equity** includes the value of tangible and intangible items, such as a brand's monetary value over time, customer perceptions and customer loyalty to a company and its products or services.[12] Businesses that already have a solid brand may find it easier to transfer their brand to the Internet, whereas Internet-only businesses must strive to develop a brand that customers trust and value.

38.4.2 Marketing Research

Marketing research can help a company develop its **marketing mix**, which includes product or service details and development, effective pricing, promotion and distribution. Traditionally, marketing research has consisted of focus groups, interviews, paper and telephone surveys, questionnaires and **secondary research** (findings based on previously

collected data). Research can now be performed over the Internet, giving marketers a new, faster channel through which to find and analyze industry, customer and competitor information. The Internet also provides a relaxed and anonymous setting on which to hold focus-group discussions and distribute questionnaires.

To target marketing campaigns effectively, it is useful to learn about the **demographics** of Internet, World Wide Web and wireless device users. Demographics are statistics on the human population, including age, sex, marital status and income. Knowledge of customers' personal information can help to reveal their purchasing preferences and buying power. Through additional research and analysis, marketers gain information about customers' **psychographics**, which can include family lifestyles, cultural backgrounds and values.[13]

Through **online focus groups**, current or potential consumers can present their opinions about products, services or ideas. This feedback can be useful when making critical decisions concerning the launch of new products, services or campaigns.

38.4.3 e-Mail Marketing

E-mail marketing campaigns provide an inexpensive and effective method of targeting potential customers. The marketer should define the **reach of a campaign**, or the span of people the marketer would like to target, including geographic locations and demographic profiles. The marketer should also determine the level of personalization of the campaign. Personalized **direct e-mail** targets consumers by using their names, offering them the right products at the right time and sending special promotions on the basis of their interests. **Internet mailing lists** can help marketers target customers through personalized e-mail. **Opt-in e-mail** is sent to people who explicitly choose to receive offers, information and promotions.[14] One popular form of opt-in e-mail is an e-newsletter that is used to keep customers up-to-date on recent products and services as well as to offer special deals and promotions to opt-in subscribers. Newsletters and other opt-in e-mails are effective tools to keep a company's target audience informed of company news without the customer having to visit the company's Web site frequently.

However, it is important to avoid flooding opt-in customers with promotional e-mail. Excessive correspondence can decrease the effectiveness of an e-mail campaign. Marketers should avoid sending e-mail to people who have not shown interest in specific products or services. **Spamming**—the distribution of mass e-mails to people who have not expressed interest in receiving information from a company—can give a company a poor reputation. (Spam is discussed in more detail in Section 38.7.4.)

38.4.4 Promotions

Promotions can both attract visitors to a site and influence purchasing. Promotions can also be used to increase brand loyalty through reward programs. Frequent-flyer miles, point-based rewards, discounts, sweepstakes, free trials, free shipping and e-coupons are all examples of promotions. Although promotions are an effective way to establish contact with potential customers, it is vital to make sure that customers are becoming loyal to the company, rather than to its promotions or rewards program. In addition, the costs of the program must be monitored carefully to make sure that a company is receiving a return on its marketing investment.

38.4.5 Consumer Tracking

While generating Web-site traffic is important to an e-business, it is not sufficient to ensure success. Keeping user profiles, recording visits and analyzing promotional and advertising results are helpful when measuring a marketing campaign's effectiveness. By discovering the **target market**—the group of people toward whom it is most profitable to aim a marketing campaign—a company can focus its campaign, increasing the number of visits, responses and purchases. Marketers use **log files** (files that contain data generated by site visits, including each visitor's location, IP address, time of visit and frequency of visits) and **log-file analysis** (the organization and summarization of information contained in log files) to monitor consumer information.

ID cards (tracking devices that provide Web sites with the numerical addresses of consumers and information regarding their operating systems) record and convey information requested by users. **Cookies**, another type of tracking device, are text files stored by Web sites on individuals' personal computers. Cookies allow a site to track the actions of a visitor. The first time a user visits a Web site, the user's computer may receive a cookie. The cookie is reactivated each time the computer revisits the site. The information collected is intended to be an anonymous account of log-on times, visit durations, purchases made on the site, the site previously visited and the site visited next. Although the cookie resides on the user's hard drive, it does not interact with other information stored on the system; furthermore, cookies can be read only by the hosts that place them.

38.4.6 Electronic Advertising

E-business advertising is conducted through such media as television, movies, newspapers and magazines, as well as online and wireless channels (wireless advertising is discussed in Section 38.12 Wireless Marketing, Advertising and Promotions). Advertising gives e-businesses the opportunity to establish and strengthen branding. The publication of URLs on all direct mailings, business cards, billboards, printed materials, wireless advertisements and other media also can increase brand awareness, bringing more visitors to a site.

While newspapers, magazines, television and films all provide effective advertising channels, the Internet is quickly becoming an important medium through which to market companies, products and services. Online advertising can include the placement of links and banners on other companies' Web sites and the registration of sites with search engines and directories. In addition, a business can obtain additional income by charging other companies for placing their advertisements on its site.

Banner advertisements are similar to billboards seen along the highway, but banners offer the additional feature of interactivity. `Valueclick.com` and `Doubleclick.com` are examples of companies that offer banner-hosting services. Some companies base advertisement charges on the number of times a banner ad is viewed on a page, whereas others charge according to the number of click-throughs generated by the banner ad. However, in both systems, advertisers pay only when a viewer clicks on the banner ad and goes to that Web site.

Pop-up ads are another form of advertising. Pop-ups appear instantly when a user visits a particular Web site. These ads are either displayed as a separate Web page launched in a browser or built into the page which a user is currently viewing. Visitors to some sites may see multiple ads appear at one time on the site they have chosen. The invasive nature of

pop-up ads can detract from the user's browsing experience, thus diminishing the return a company can get on the ad's effectiveness.

Search engine "pay-for-performance" advertising has become a billion-dollar industry and is one of the fastest-growing forms of advertising on the Web.[15] (Search engines are discussed in the next section.) Popular search engines such as Google, Overture, Yahoo!, MSN, AOL, and Earthlink allow businesses to purchase keywords that best describe their products or services (e.g., IT consulting, gardening, e-business solutions). Then, when a consumer searches for those keywords, relevant Web links that best match the keywords are returned along with additional advertising links ranked according to the highest bidder for those specific keywords. If a user clicks on a company's ad, then the company is charged based on the number of click-throughs to its site generated by that ad. In turn, search engines monitor the number of times users actually click on a company's add to determine its effectiveness and performance. If a company's ad is not performing well, then its ranking is lowered (regardless of what it bid on the keywords) and other companies that have bid on the same keywords advance upwards in the rankings. This advertising structure is common for some search engines and others use different formulas to determine performance and ranking position of ads.

38.4.7 Search Engines

A **search engine** is a program that scans Web sites for desired content, listing relevant sites on the basis of keywords or other search-engine ranking criteria. **Search-engine ranking** is an important way to bring new visitors to a site. The method used by a search engine to rank a Web site will determine how close to the top a site appears on lists of search results. Businesses can customize and register their sites to improve their positions in search-engine results (see the Google feature).

Google: The Technology Behind Today's Search Engines

The Web has become one of the most important tools we use to obtain information quickly and easily. Whether it is searching for research materials on a particular topic or finding local theaters playing our favorite movies, we use the Web to find answers to almost any question we may have, big or small. There are many search engines available to assist users in their searches, including such popular sites as `www.google.com`, `www.yahoo.com`, `www.alltheweb.com` and `www.altavista.com`. However, the search process is far from perfect. Users may wish to find certain information on a particular subject, but the search engine may return results that are not relevant or useful to them.

Most search engines companies are looking for ways to make Internet searches more accurate and useful to the user. Some search engines use spiders that crawl the Web looking through thousands of Web pages for keywords that match the keywords entered by the user making a search request. Other companies, such as Google, take a more scientific approach to the concept of search.

Google: The Technology Behind Today's Search Engines (Cont.)

Google is one of the most popular search engines used to find information on the Web. It currently performs 33% of all English-based global searches worldwide.[16] Google and other search engines continue to take the technology behind search to new levels in a process of continuous improvement. Google uses complex mathematical formulas that rank relevant Web pages based on factors such as the number of other Web pages that link to the site, page views, click-throughs and more. For examples if a Web page contains keywords from a user's search, the site is marked, and how many other Web sites reference this page is also noted. The more pages that reference it, the higher the number value Google assigns to it as part of its search formula. Google then calculates the results and returns the Web pages ranked in order of relevancy to the user.

Users want answers to their questions quickly, so Google relies on 15,000 servers that search over 3 billion Web pages simultaneously to display results to the user in approximately 0.02 seconds per search.[17] While 3 billion Web pages may seem quite large, it is actually just one small portion of the Web. For Google and other search engines, the challenge still remains to search more of the untapped Web at still faster speeds and produce even more accurate results to further enhance each user's search experience.

A **meta tag** is an XHTML tag that contains information about a Web page. Although the tag does not change how a Web page is displayed, it can contain a description of the page, keywords and the page's title. Search engines often use meta-tag information when ranking a site.

Some search engines rank sites by sending out a program, called a **spider**, to inspect each site. The spider reads the meta tags, determines the relevance of the Web page's information and keywords and then ranks the site according to the visit's findings. Marketers should examine competitors' sites, analyzing their' meta tags and content. It is important to have a site appear in the top results, because often people will not look further. For valuable information about keyword selection, visit `www.keywordcount.com` and `www.websearch.about.com/internet/websearch/insub2-m02.htm`.

38.4.8 Affiliate Programs

Affiliate programs have become a dominant and unique form of Internet marketing. An affiliate program is a form of partnership in which a company pays **affiliates** (other companies or individuals) on the basis of prespecified actions by visitors who **click-through** from an **affiliate site** to a **merchant site**.

Affiliate programs also can increase Web-site traffic. Affiliates post links on each other's sites in exchange for referral fees, which usually consist of a percentage of each sale or a fixed fee for click-throughs that result in sales. `Befree.com` is a fee-based service that helps users set up affiliate programs. For more information, visit `www.befree.com`. Another popular example is `Amazon.com`'s affiliate program. Users can post links from their sites to books and products available for sale on Amazon. If a visitor to Amazon's site then purchases a linked product, the Web-site host through which the user clicked to get to

Amazon's site receives a small payment. If the user does not purchase the product for which he or she originally clicked through to Amazon, but purchases another product while still browsing the site, the Web-site host receives a percentage of the purchase amount as a referral fee. If a user only views a product, then returns to `Amazon.com` directly at a later time to purchase the product, no one receives referral fees for this purchase.

38.4.9 Public Relations

Public relations (**PR**) provides customers and employees with the latest information about products, services and such issues as company promotions and consumer reactions. A vital aspect of public relations is communication with customers and employees through press releases, speeches, special events, presentations and e-mail.

Press releases, which announce current events and other significant news to the press, can be delivered over the Web. For example, PR Web (`www.prweb.com`) allows marketers to submit press releases to its site for free. Online press releases sometimes include video clips of news appearances, speeches, commercials and advertisements, all of which can be effective publicity. Visit `www.prnewswire.com` and `www.businesswire.com` to view lists of recent press releases, including audio and video news.

Crisis management, an aspect of PR, is conducted in response to problems a company is experiencing. When a company is doing poorly, its public-relations department will often issue information regarding the causes and announce what steps will be implemented to remedy the problem.

38.4.10 Customer Relationship Management (CRM)

Customer relationship management (**CRM**) focuses on the provision and maintenance of quality service for customers. Effective CRM involves communicating with customers and delivering products, services, information and solutions in response to their problems, wants and needs. Customer satisfaction is key to business success, because it is far less expensive to keep current customers than to acquire new ones. Online businesses should give particular attention to CRM, because transactions are often conducted through a series of third parties, and thus the establishment of personal relationships with customers requires innovative strategies.

Aspects of CRM are **call handling** (the maintenance of outbound and inbound calls from customers and service representatives), **sales tracking** (the tracking and recording of all sales made) and **transaction support** (support for technology and personnel involved in business transactions). Unique functions of eCRM, the application of CRM to an e-business strategy, include the personalization and customization of customers' experiences and interactions with a Web site, call center or any other forum for customer contact with the e-business. The term iCRM (Internet customer relationship management) can be used interchangeably with eCRM in reference to e-business customer relationship management. Business analysts should review all CRM plan details and data, such as reductions in costs or an influx of customer complaints, to refine the CRM system.

e-Fact 38.2

According to the Boston Consulting Group, the cost of acquiring a new online customer is approximately $34, whereas marketing to a current customer through the Internet costs around $7.[18]

38.5 Online Payments

Secure electronic funds transfer (EFT) is crucial to e-commerce. Credit-card payments, digital cash and e-wallets, smart cards, micropayments and electronic bill presentment and payment are methods for conducting online transactions. Many companies offer products, software and services that enable monetary transactions on the Web.

38.5.1 Credit-Card Payment

Although credit cards are a popular form of online payment, many people resist online credit-card transactions because of security concerns. Customers fear credit-card fraud by merchants and third parties. However, most credit cards, such as Visa®, Mastercard® and American Express®, have features that enable secure online and offline payments.

To accept credit-card payments, a merchant must have a **merchant account** with a bank. Traditional merchant accounts accept only **point-of-sale (POS) transactions**, that is, transactions that occur when customers present credit cards at stores. However, the growth of e-commerce has resulted in the establishment of specialized Internet merchant accounts that handle online credit-card transactions. These consist of **card-not-present (CNP)** transactions. For example, when users make credit-card purchases through the Internet, they can provide the card numbers and expiration dates, but the merchant does not see the actual cards involved in the transactions. A merchant account can be established through either a bank or a third-party service.[19]

38.5.2 Digital Cash and e-Wallets

Digital cash is one example of digital currency. It is stored electronically and can be used to make online electronic payments. Digital-cash accounts are similar to traditional bank accounts; consumers deposit money into digital-cash accounts for use in digital transactions. Often, digital cash is used in conjunction with other payment technologies, such as digital wallets. In addition to providing a payment alternative for customers with security concerns regarding online credit-card transactions, digital cash allows people who do not have credit cards to shop online (see the PayPal feature).

PayPal, Inc.

PayPal (`www.paypal.com`) was founded in 1998 as an intermediate solution for users purchasing products and services online. PayPal allows customers to conduct transactions on the Internet quickly and easily without any need to submit credit-card or back account information every time they wish to spend money on the Web.

To use PayPal, users are required to establish an account using a credit card or backed by their account at a financial institution. Once an account is set up, users can, among other things, purchase products or services online, pay bills, and transfer money to other people via PayPal's partner Web sites. PayPal currently has over 30 million users in 38 different countries and is one of the leading businesses that conduct and control online payment.[20]

eBay, the largest auction site on the Internet, purchased PayPal in October 2002 for $1.5 billion. eBay now uses PayPal to conduct its auction transactions over the Internet.[21]

To facilitate the credit-card order process, many companies are introducing **electronic wallet** services. **E-wallets** keep track of billing and shipping information so that it can be entered with one click at participating merchants' sites. E-wallets also store e-checks, e-cash and credit-card information for multiple cards.

38.5.3 Micropayments

Merchants are required to pay a fee for each credit-card transaction they process, which becomes costly when customers purchase inexpensive items. Sometimes, the cost of an item is actually lower than the standard transaction fee, causing the merchant to incur losses. **Micropayments** (payments that generally do not exceed $5) enable ways for nominally priced products and services (e.g., music, pictures, texts or videos) to be sold profitably over the Web. For instance, a phone bill is essentially an aggregation of micropayments that are charged periodically at set intervals to justify the transaction fee. To offer micropayment processing, some companies have formed strategic partnerships with telephone carriers and utility companies.

In 2002, content purchased through micropayments grew faster than any other category of fee-based content, as sales grew ten times over the previous year to $3 million, and spending for content in the third quarter of 2002 alone was up 132% over the preceding year to $56 million.[22]

e-Fact 38.3

According to an ongoing study conducted by the Gartner Group, only a small percentage of online retailers offer a payment option for items priced under $10.[23]

38.5.4 Smart Cards

A smart card generally looks like a credit card and can serve many different functions, from authentication to data storage. The most popular smart cards are **memory cards** and **microprocessor cards**. Memory cards are similar to floppy disks. Microprocessor cards are similar to small computers, with operating systems, security and storage. Smart cards also have different **interfaces** with which they interact with reading devices. One type of interface is a **contact interface**, in which a smart card is inserted into a reading device and physical contact between the device and the card is necessary (For example American Express®'s Blue). The alternative to this method is a **contactless interface**, in which data is transferred to a reader via an embedded wireless device in the card, without the card and the device having to make physical contact.[24]

Contactless cards are convenient for transportation services, such as automatic toll payments. A contactless smart card, when placed in a device in a car, will charge the user's account as he or she drives through toll booths (such as FAST LANE®, E-ZPass℠ used in Massachusetts and New York, respectively and FasTRAK™ used in California).[25]

Smart cards store credit-card numbers, personal contact information, and so on. Each smart card is used in combination with a **personal identification number** (**PIN**). This application provides two levels of security by requiring the user to both possess a smart card and know the corresponding PIN to access the information stored on the card. As an added measure of security, some microprocessor cards will delete or corrupt stored data if malicious attempts at tampering with the card occur. In addition, smart cards can require users to enter passwords, thus offering a higher level of security than credit cards. Informa-

tion maintained on smart cards can be designated as "read only" or as "no access." The cards can also be enhanced with additional security features, such as encryption and photo identification.

38.6 Security

As e-businesses and Web services (Web services are discussed in Chapter 20 and Chapter 23) gain widespread adoption, individuals and organizations are transmitting highly confidential information over the Internet. Consumers are submitting credit-card numbers to e-commerce sites, and businesses are exposing proprietary data on the Web. At the same time, organizations are experiencing increasing numbers of security breaches. Both individuals and companies are vulnerable to data theft and hacker attacks that can compromise data, corrupt files and crash systems. For these reasons, security is crucial to the success of e-businesses. In a memo to all Microsoft employees, Bill Gates stated that the company's highest priority is trustworthy computing—that is ensuring that Microsoft applications are reliable, available and secure. Gates's security emphasis has been echoed across the computing industry as organizations work to improve Internet and network security.[26]

There are five fundamental requirements for a successful, secure transaction: **privacy**, **integrity**, **authentication**, **authorization** and **nonrepudiation**. *The privacy issue is:* How do you ensure that the information you transmit over the Internet has not been captured or passed to a third party without your knowledge? *The integrity issue is*: How do you ensure that the information you send or receive has not been compromised or altered? *The authentication issue is*: How do the sender and receiver of a message verify their identities to each other? *The authorization issue is*: How do you manage access to protected resources on the basis of user credentials? *The nonrepudiation issue is*: How do you legally prove that a message was sent or received? Network security must also address the issue of **availability**. How do we ensure that the network, and the computer systems to which it connects, will operate continuously?

In this section, we explore the fundamentals of Internet security, including secure electronic transactions and secure networks. We discuss how to achieve e-commerce and network security using current technologies—including cryptography, Public Key Infrastructure (PKI), digital signatures, Secure Sockets Layer (SSL) and Virtual Private Networks (VPNs). We also examine authentication and authorization solutions, firewalls and intrusion-detection systems.

38.6.1 Public-Key Cryptography

The channels through which data passes are not secure; therefore, any private information transmitted through these channels must be protected. To secure information, data can be encrypted. **Cryptography** transforms data by using a **cipher**, or **cryptosystem** (a mathematical algorithm for the encryption of messages). Algorithm is a computer science term for a "procedure." A **key** (a string of digits or letters that acts as a password in the cipher) makes the data incomprehensible to everyone but the sender and intended recipients. Unencrypted data is known as **plain text**, whereas encrypted data is called **ciphertext**. Only the intended recipients should possess the corresponding key to decrypt the ciphertext into plaintext.

Formerly, organizations that wished to maintain a secure computing environment used **symmetric cryptography**, also known as **secret-key cryptography**. Secret-key cryptog-

raphy uses the same secret key to encrypt and decrypt a message. When employing such cryptography, the sender encrypts a message using the secret key, then sends the encrypted message and the symmetric secret key to the intended recipient. However, problems with this method arise because, before two people can communicate securely, they must find a secure way to exchange the secret key. The privacy and integrity of the message could be compromised if the key is intercepted as it is transmitted from sender to recipient over unsecure channels. In addition, since both parties in the transaction use the same key to encipher and decipher a message, it is impossible to authenticate which party created the message.

In 1976, Whitfield Diffie and Martin Hellman, researchers at Stanford University, developed **public-key cryptography** to solve the problem of exchanging keys securely. Public-key cryptography is asymmetric. It uses two inversely related keys: a **public key** and a **private key**. The private key is kept secret by its owner, whereas the public key is freely distributed. If the public key is used to encrypt a message, only the corresponding private key can decrypt it (Fig. 38.3). Each party in a transaction has both a public key and a private key. To transmit a message securely, the sender uses the receiver's public key to encrypt the message. The receiver then decrypts the message using his or her unique private key. Assuming that the private key has been kept secret, the message cannot be read by anyone other than the intended receiver. Thus the system ensures the privacy of the message. The defining property of a secure public-key algorithm is that it is "computationally infeasible" to deduce the private key from the public key. Although the two keys are mathematically related, deriving one from the other would take enormous amounts of computing power and time, enough to discourage attempts to deduce the private key. An outside party cannot participate in communication without the correct keys. The security of the entire process is based on the secrecy of the private keys. Therefore, if a third party obtains the private key used in decryption, the security of the whole system is compromised. If a system's integrity is compromised, the user can simply change the key, instead of changing the entire encryption or decryption algorithm.

Digital signatures, the electronic equivalent of written signatures, are used in public-key cryptography to solve authentication and integrity problems. A digital signature authenticates the sender's identity, and, like a written signature, it is difficult to forge. To create a digital signature, a sender first runs a plaintext message through a **hash function**, which is a mathematical calculation that gives the message a **hash value**. For example, you could take the plaintext message "Buy 100 shares of company X," run it through a hash function and get a hash value of 42. The hash function could be as simple as adding up all the 1s in a message, although it is usually more complex. The hash value is also known as a **message digest**. The chance that two different messages will have the same message digest is statistically insignificant. **Collision** occurs when multiple messages have the same hash value. However, it is computationally infeasible to compute a message from its hash value or to find two messages with the same hash value for hash algorithms commonly used today.

Either the public key or the private key can be used to encrypt or decrypt a message. For example, if a customer uses a merchant's public key to encrypt a message, only the merchant can decrypt the message, using the merchant's private key. Thus, the merchant's identity can be authenticated, since only the merchant knows the private key. However, the merchant has no way of validating the customer's identity, since the encryption key the customer used is publicly available.

Fig. 38.3 Encrypting and decrypting a message using public-key cryptography.

These two methods of public-key encryption can be used together to authenticate both participants in a communication (Fig. 38.4). Suppose a merchant wants to send a message securely to a customer so that only the customer can read it, and suppose also that the merchant (not an unknown third party)

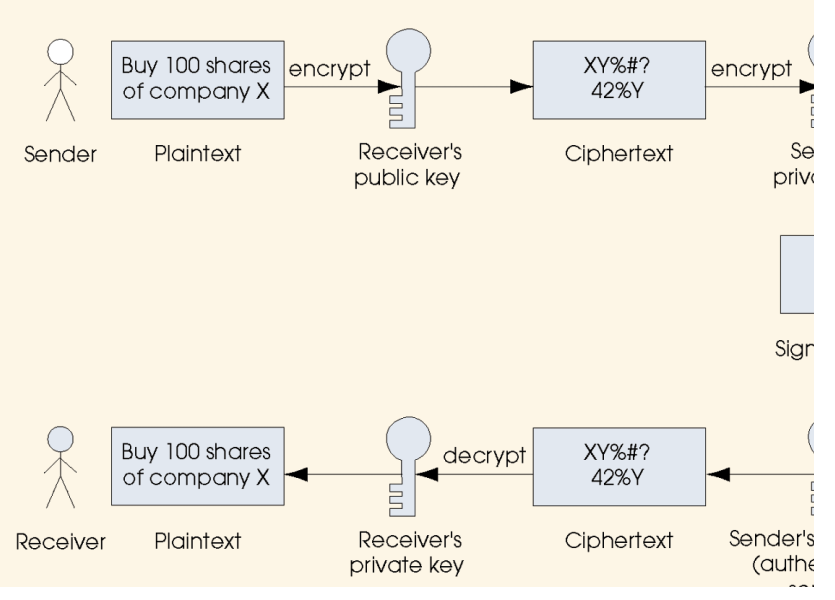

Fig. 38.4 Authentication with a public-key algorithm.

actually sent the message. First, the merchant encrypts the message using the customer's public key. This step guarantees that only the customer can read the message. Then the merchant encrypts the result using the merchant's private key, which proves the identity of the merchant. The customer decrypts the message in reverse order. First, the customer uses the merchant's public key. Since only the merchant could have encrypted the message with the inversely related private key, this step authenticates the merchant. Then the customer uses the customer's private key to decrypt the next level of encryption. This step ensures that the content of the message was kept private in the transmission, since only the customer has the key to decrypt the message. Although this system provides extremely secure transactions, the setup cost and time required discourage widespread use.

One problem with public-key cryptography is that anyone with a set of keys could potentially assume another party's identity. For example, imagine that a customer wants to place an order with an online merchant. How does the customer know that the Web site indeed belongs to that merchant and not to a third party who is masquerading as the merchant to steal credit-card information? **Public Key Infrastructure** (**PKI**) integrates public-key cryptography with **digital certificates** and **certificate authorities** to authenticate parties in a transaction. **Wireless PKI** (**WPKI**) is a security protocol specifically for wireless transmissions. Like regular PKI, WPKI authenticates users via digital certificates and encrypts messages using public-key cryptography. The system also ensures nonrepudiation.

Digital certificates are digital documents issued by a **certification authority** (**CA**). A digital certificate includes the name of the subject (the company or individual being certified), the subject's public key, a serial number, an expiration date, the signature of the trusted certification authority and any other relevant information. A CA is a financial institution or other trusted third party, such as **VeriSign**. Because the CA assumes responsibility for authentication, it must check information carefully before issuing a digital certificate. Once issued, digital certificates are publicly available and are held by the certification authority in **certificate repositories**. VeriSign, Inc., is a leading certification authority. (To learn more about VeriSign, visit `www.verisign.com`.)

Many people still consider e-commerce to be unsecure. However, transactions using PKI and digital certificates are more secure than point-of-sale credit-card purchases or the exchange of private information over phone lines or through the mail. The key algorithms used in most secure online transactions are nearly impossible to compromise. By some estimates, the key algorithms used in public-key cryptography are so secure that a century would pass before millions of today's computers working in parallel could break the codes.

The most commonly used public-key algorithm is **RSA**, an encryption system developed in 1977, and named for its creators, MIT professors Ron Rivest, Adi Shamir and Leonard Adleman.[27] Today, most Fortune 1000 companies and leading e-commerce businesses use their encryption and authentication technologies. With the emergence of the Internet and the World Wide Web, their security work has become even more significant and plays a crucial role in e-commerce transactions. Their encryption products are built into hundreds of millions of copies of the most popular Internet applications, including Web browsers, commerce servers and e-mail systems. Most secure e-commerce transactions and communications on the Internet use RSA products. For more information about RSA, cryptography and security, visit `www.rsasecurity.com`. Other organizations, such as Microsoft, also offer products to ensure security. (See the Microsoft Authenticode feature.)

Microsoft Authenticode: Authenticating Software

How do you know that the software you ordered online is safe and has not been altered? How can you be sure that you are not downloading a computer virus that could wipe out your computer? Do you trust the source of the software? With the emergence of e-commerce, software companies are offering their products online, so that customers can download software directly onto their computers. Security technology is used to ensure that the downloaded software is trustworthy and has not been altered. *Microsoft Authenticode*, combined with VeriSign digital certificates (or **digital IDs**), authenticates the publisher of the software and detects whether the software has been altered. Authenticode is a security feature built into Microsoft Internet Explorer.

To use Microsoft Authenticode technology, a software publisher must obtain a digital certificate specifically designed for the purpose of publishing software; such certificates may be obtained through certificate authorities, such as VeriSign. To obtain a certificate, a software publisher must provide its public key and identification information and sign an agreement that it will not distribute harmful software. This requirement gives customers legal recourse if any downloaded software from a certified publisher causes harm.

Microsoft Authenticode uses digital-signature technology to sign software. The signed software and the publisher's digital certificate provide proof that the software is safe and has not been altered.

When a customer attempts to download a file, a dialog box appears on the screen displaying the digital certificate and the name of the certificate authority. Links to the publisher and the certificate authority are provided so that customers can learn more about each party before they agree to download the software. If Microsoft Authenticode determines that the software has been compromised, the transaction is terminated.

To learn more about Microsoft Authenticode, visit the following sites:

```
msdn.microsoft.com/workshop/security/authcode/signing.asp
msdn.microsoft.com/workshop/security/authcode/authenticode.asp
```

Pretty Good Privacy (**PGP**) is a public-key encryption system for encrypting e-mail messages and files. PGP was designed in 1991 by Phillip Zimmermann.[28] PGP can also be used to provide digital signatures that confirm the author of an e-mail or public posting.

PGP is based on a "web of trust"; each client in a network can vouch for another client's identity to prove ownership of a public key. The web of trust is used to authenticate each client. If users know the identity of a public key holder, through personal contact or another secure method, they validate the key by signing it with their own key. The web grows as more users validate the keys of others. To learn more about PGP and to download a free copy of the software, go to the MIT Distribution Center for PGP at `web.mit.edu/network/pgp.html`.

38.6.2 Cryptanalysis

Even if keys are kept secret, it may be possible to compromise the security of a system. Trying to decrypt ciphertext without knowledge of the decryption key is known as **cryptanal-**

ysis. Cryptologists are constantly researching commercial encryption systems to ensure that the systems are not vulnerable to a **cryptanalytic attack**. The most common form of cryptanalytic attacks are those in which the encryption algorithm is analyzed to find relations between bits of the encryption key and bits of the ciphertext. Often, these relations are only statistical in nature and incorporate an analyzer's outside knowledge about the plaintext. The goal of such an attack is to determine the key from the ciphertext.

Weak statistical trends between ciphertext and keys can be exploited to gain knowledge about the key if enough ciphertext is known. Proper key management and key expiration dates on keys help prevent cryptanalytic attacks. When a key is used for long periods of time, more ciphertext is generated that can be beneficial to an attacker trying to derive the key. If a key is unknowingly recovered by an attacker, it can be used to decrypt every message for the life of that key. Using public-key cryptography to exchange secret keys securely allows a new secret key to encrypt every message.

38.6.3 Key Agreement Protocols

A drawback of public-key algorithms is that they are not efficient for sending large amounts of data. They require significant computer power, which slows communication. Public-key algorithms should not be thought of as replacements for secret-key algorithms. Instead, public-key algorithms are used most often to exchange secret keys securely. The process by which two parties can exchange keys over an unsecure medium is called a **key agreement protocol**. A **protocol** sets the rules for communication—for example, which encryption algorithm(s) to use.

The most common key agreement protocol is a **digital envelope** (Fig. 38.5). With a digital envelope, the message is encrypted using a secret key (Step 1), and the secret key is encrypted using public-key encryption (Step 2). The sender attaches the encrypted secret key to the encrypted message and sends the receiver the entire package. The sender could also digitally sign the package before sending it to prove the sender's identity to the receiver. To decrypt the package, the receiver first decrypts the secret key using the receiver's private key. Then the receiver uses the secret key to decrypt the actual message. Since only the receiver can decrypt the encrypted secret key, the sender can be sure that only the intended receiver is reading the message.

38.6.4 Key Management

Maintaining the secrecy of private keys is crucial for keeping cryptographic systems secure. Most compromises in security result from poor **key management** (e.g., the mishandling of private keys, resulting in key theft) rather than attacks that attempt to guess the keys.[29]

A main component of key management is **key generation**—the process by which keys are created. A malicious third party could try to decrypt a message by using every possible decryption key, a process known as **brute-force cracking**. Key-generation algorithms are sometimes unintentionally constructed to choose from only a small subset of possible keys. If the subset is too small, then the encrypted data is more susceptible to brute-force attacks. Therefore, it is important to have a key-generation program that can generate a large number of keys as randomly as possible. Keys are made more secure by choosing a key length so large that it is computationally infeasible for a malicious third party to try all combinations.

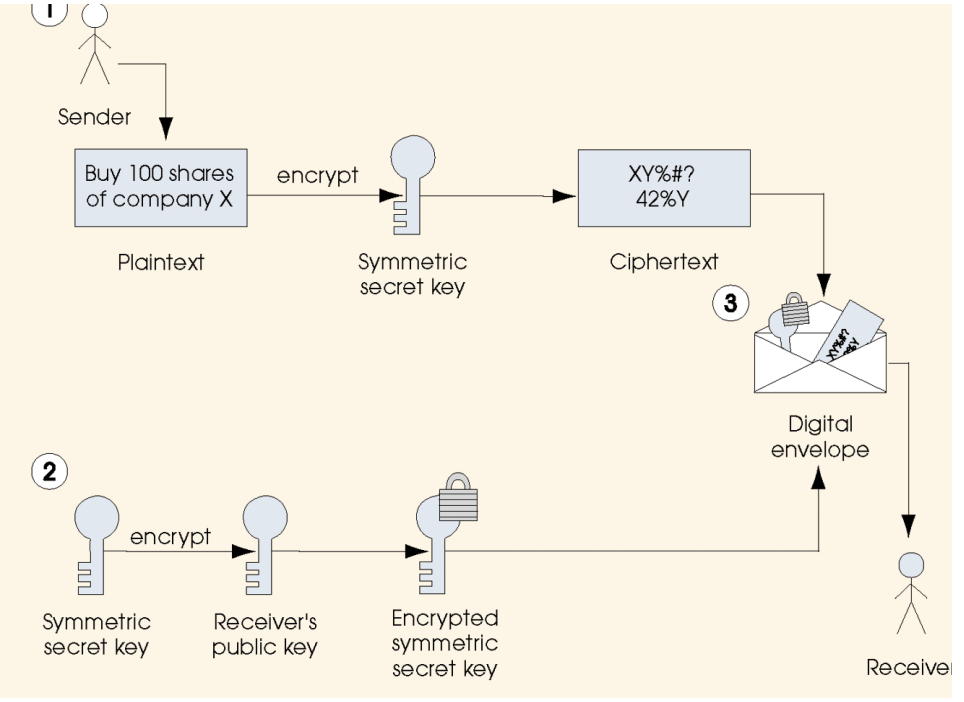

Fig. 38.5 Creating a digital envelope.

38.6.5 Secure Sockets Layer (SSL)

Currently, most e-businesses use SSL for secure online transactions, although SSL is not designed specifically for securing transactions. Rather, SSL secures World Wide Web connections. The Secure Sockets Layer (SSL) protocol, developed by Netscape Communications, is a non-proprietary protocol commonly used to secure communication between two computers on the Internet and the Web.[30] SSL is built into many Web browsers, including Netscape Communicator and Microsoft Internet Explorer, as well as numerous other software products. It operates between the Internet's TCP/IP communications protocol and the application software.[31]

In a standard correspondence over the Internet, a sender's message is passed to a **socket**, which receives and transmits information from a network. The socket then interprets the message through **Transmission Control Protocol/Internet Protocol** (**TCP/IP**). TCP/IP is the standard set of protocols used for connecting computers and networks to a network of networks, known as the Internet. Most Internet transmissions are sent as sets of individual message pieces, called **packets**. On the sending side, the packets of one message are numbered sequentially, and error-control information is attached to each packet. IP is primarily responsible for routing packets to avoid traffic jams, so each packet might travel a different route over the Internet. The destination of a packet is determined by the **IP address**—an assigned number used to identify a computer on a network, similar to the address of a house in a neighborhood. At the receiving end, the TCP makes sure that all of

the packets have arrived, puts them in sequential order and determines whether the packets have arrived without alteration. If the packets have been accidentally altered or any data has been lost, TCP requests retransmission. However, TCP is not sophisticated enough to determine whether packets have been maliciously altered during transmission, because malicious packets can be disguised as valid ones. When all of the data successfully reaches TCP/IP, the message is passed to the socket at the receiver end. The socket translates the message back into a form that can be read by the receiver's application.[32] In a transaction using SSL, the sockets are secured using public-key cryptography.

SSL implements public-key cryptography using the RSA algorithm and digital certificates to authenticate the server in a transaction and to protect private information as it passes over the Internet. SSL transactions do not require client authentication; many servers consider a valid credit-card number to be sufficient for authentication in secure purchases. To begin, a client sends a message to a server. The server responds and sends its digital certificate to the client for authentication. Using public-key cryptography to communicate securely, the client and server negotiate **session keys** to continue the transaction. Session keys are secret keys that are used for the duration of a single transaction. Once the keys are established, the communication proceeds between the client and the server by using the session keys and digital certificates. Encrypted data is passed through TCP/IP, just as regular packets travel over the Internet. However, before sending a message with TCP/IP, the SSL protocol breaks the information into blocks, compresses it and encrypts it. Conversely, after the data reaches the receiver through TCP/IP, the SSL protocol decrypts the packets, then decompresses and assembles the data. These extra processes provide an extra layer of security between TCP/IP and applications. SSL is primarily used to secure **point-to-point connections**—transmissions of data from one computer to another.[33] SSL allows for authentication of the server, the client, both or neither. However, in most e-business SSL sessions, only the server is authenticated. The Transport Layer Security (TLS) protocol, designed by the Internet Engineering Task Force, is similar to SSL. For more information on TLS, visit `www.ietf.org/rfc/rfc2246.txt`.

Although SSL protects information as it is passed over the Internet, it does not protect private information, such as credit-card numbers, once the information is stored on the merchant's server. When a merchant receives credit-card information with an order, the information is often decrypted and stored on the merchant's server until the order is placed. If the server is not secure and the data is not encrypted, an unauthorized party can access the information. Hardware devices, such as **peripheral component interconnect (PCI) cards** designed for use in SSL transactions, can be installed on Web servers to process SSL transactions, thus reducing processing time and leaving the server free to perform other tasks.[34] Visit `www.sonicwall.com/products/trans.asp` for more information on these devices. For more information about the SSL protocol, check out the Netscape SSL tutorial at `developer.netscape.com/tech/security/ssl/protocol.html` and the Netscape Security Center site at `www.netscape.com/security/index.html`.

38.6.6 WTLS

Wireless Transport Layer Security (**WTLS**) is the security protocol for the **Wireless Application Protocol** (**WAP**). WAP is a standard used for wireless communications on mobile phones and other wireless devices. WTLS secures connections between wireless devices and application servers. It provides wireless technology with data integrity, priva-

cy, authentication and denial-of-service security. WTLS encrypts data sent between a WAP-enabled wireless device and a WAP **gateway,** where messages are transferred from the wireless network to a wired network. At the gateway, data is decrypted from WTLS and subsequently encrypted into SSL. For a few milliseconds, the data is not encrypted and, therefore, unsecure. The brief lapse in security is called the **WAP gap**. Although this flaw causes the system to be unsecure, it is extremely difficult to exploit the WAP gap in practice. No one has ever reported an attack on the WAP gap that has successfully caused the compromise of any secure data.

38.6.7 IPSec and Virtual Private Networks (VPNs)

Networks allow organizations to link multiple computers together. **Local area networks** (**LANs**) connect computers that are physically close, generally in the same building. **Wide area networks** (**WANs**) are used to connect computers in multiple locations using private telephone lines or radio waves. Organizations are now taking advantage of the existing infrastructure of the Internet—the publicly available wires—to create **Virtual Private Networks** (**VPNs**). VPNs connect multiple networks, wireless users and other remote users. VPNs use the Internet infrastructure that is already in place, therefore they are more economical than private networks such as WANs.[35] Encryption allows VPNs to provide the same services as private networks do—over a public network.

A VPN is created by establishing a secure **tunnel** through which data passes between multiple networks over the Internet. **IPSec** (**Internet Protocol Security**) is one of the technologies used to secure the tunnel through which the data passes, ensuring data privacy and integrity, as well authenticating users.[36]

IPSec, developed by the **Internet Engineering Task Force** (**IETF**), uses public-key and symmetric-key cryptography to ensure data integrity, authentication and confidentiality. The technology takes advantage of the standard that is already in place, in which information travels between two networks over the Internet via the **Internet Protocol** (**IP**). Information sent using IP, however, can easily be intercepted. Unauthorized users can access the network by using a number of well-known techniques, such as **IP spoofing**—a method in which an attacker simulates the IP of an authorized user or host to get access to resources that would otherwise be off-limits. The SSL protocol enables secure point-to-point connections between two applications; IPSec enables the secure connection of an entire network. The Diffie-Hellman and RSA algorithms are commonly used in the IPSec protocol for key exchange, and DES or 3DES is used for secret-key encryption (depending on system and encryption needs). An IP packet is encrypted, then sent inside a regular IP packet that creates the tunnel. The receiver discards the outer IP packet, then decrypts the inner IP packet.[37] VPN security relies on three concepts—authentication of the user, encryption of the data sent over the network and controlled access to corporate information.[38]

To address these three security concepts, IPSec is composed of three parts. The **Authentication Header** (**AH**) attaches additional information to each packet, which verifies the identity of the sender and proves that data was not modified in transit. The **Encapsulating Security Payload** (**ESP**) encrypts the data using symmetric key ciphers to protect the data from eavesdroppers while the IP packet is being sent from one computer to another. The **Internet Key Exchange** (**IKE**) is the key-exchange protocol used in IPSec to determine security restrictions, authenticate the encryption keys and establish the tunnels.

VPNs are becoming increasingly popular in businesses. However, VPN security is difficult to manage. To establish a VPN, all of the users on the network must have similar software or hardware. Although it is convenient for a business partner to connect to another company's network via VPN, access to specific applications and files should be limited to authorized users versus all users on a VPN.[39] Firewalls, intrusion-detection software and authorization tools can be used to secure valuable data. For more information about IPSec, visit the IETF's *IPSec Working Group* Web site (`www.ietf.org/html.charters/ipsec-charter.html`).

38.6.8 Security Attacks

Recent cyberattacks on e-businesses have made the front pages of newspapers worldwide. **Denial-of-service** (**DoS**) **attacks**, **viruses** and **worms** have cost companies billions of dollars. Typically, a denial-of-service attack occurs when a network or server is flooded with data packets. The influx of data greatly increases the traffic on the network, overwhelming the servers and making it impossible for legitimate users to download information. A **distributed denial-of-service attack** occurs when an unauthorized user gains illegitimate control of a network of computers (usually by installing viruses on them), then all the computers simultaneously attack a single target. These attacks cause networked computers to crash or disconnect from the network, making services unavailable for legitimate users.

Viruses are computer programs—often sent as e-mail attachments or disguised as audio clips, video clips and games—that attach to or overwrite other programs in order to replicate themselves. Viruses can corrupt files or even wipe out a hard drive. The spread of a virus occurs through sharing "infected" files embedded in e-mail attachments, documents or programs. Worms are similar to viruses, but a worm can spread and infect files on its own over a network; worms do not need to be attached to another program to spread. Two of the most famous viruses to date are **ILOVEYOU,** launched in May 2000, and **CodeRed**, which hit in late 2001, both cost organizations and individuals billions of dollars. The **Blaster worm**, which struck in August 2003, had an equally detrimental effect worldwide. Viruses and worms are not limited to computers. In June 2000, a worm named **Timofonica** that was propagated through e-mail quickly made its way into the cell-phone network in Spain, sending prank calls and leaving text messages on subscribers' phones.[40]

Who is responsible for viruses and denial-of-service attacks? Most often the responsible parties are referred to as **hackers** or **crackers**. Hackers and crackers are usually skilled programmers. According to some, hackers break into systems just for the thrill of it, without causing harm to the compromised systems, whereas crackers have malicious intent. However, regardless of an attack's consequences, hackers and crackers break the law by accessing or damaging private information and computers. Many vendors offer antivirus utilities that help protect computers against viruses and other threats. For more information on such protection features, visit McAfee at `www.mcafee.com` and Symantec at `www.symantec.com` (see the `McAfee.com` feature).

38.6.9 Network Security

The goal of network security is to allow authorized users access to information and services while preventing unauthorized users from gaining access to, and possibly corrupting, the network. A basic tool used in network security is the **firewall**, which protects a **local area**

McAfee.com: Antivirus Utilities

McAfee.com provides a variety of antivirus utilities (and other utilities) for users whose computers are not continuously connected to a network, for users whose computers are continuously connected to a network (such as the Internet) and for users connected to a network via wireless devices, such as personal digital assistants.

For computers that are not continuously connected to a network, McAfee provides its antivirus software *VirusScan*®. This software is configurable to scan files for viruses on demand or to scan continuously in the background as the user does his or her work.

For computers that are network and Internet accessible, McAfee provides its online **McAfee.com** Clinic. Users with a subscription to McAfee Clinic can use the online virus software from any computer they happen to be using. As with VirusScan software on stand-alone computers, users can scan their files on demand. A major benefit of the Clinic is its *ActiveShield* software. Once installed, ActiveShield can be configured to scan every file that is used on the computer or just the program files. It can also be configured to check automatically for virus definition updates and notify the user when such updates become available. The user simply clicks on the supplied hyperlink in an update notification to connect to the Clinic site and clicks on another hyperlink to download the update. Thus, users can keep their computers protected with the most up-to-date virus definitions at all times, an important factor in protection from viruses.

McAfee.com *VirusScan Wireless* provides virus protection for Palm™ handhelds, Pocket PC and other handheld devices. VirusScan Wireless is installed on the user's PC. Each time the user syncs the handheld device, the software scans for viruses. If a virus is detected, the sync is terminated until the user deletes the virus. For more information about McAfee, visit `www.mcafee.com`. Also check out Norton security products from Symantec, at `www.symantec.com`. Symantec is a leading security software vendor. Its product, Norton™ Internet Security 2004, provides protection against hackers, viruses and threats to privacy for both small businesses and individuals.

network (**LAN**) from intruders outside the network. For example, most companies have internal networks that allow employees to share files and access company information. Each LAN can be connected to the Internet through a gateway, which usually includes a firewall. A firewall acts as a safety barrier for data flowing into and out of the LAN. Firewalls can prohibit all data flow that is not expressly allowed, or they can allow all data flow that is not expressly prohibited. Although network security administrators can choose freely between these options, decisions should weigh the need for security against the need for functionality. A personal firewall can be used to protect a single PC.

What happens if a hacker gets inside a firewall? How does a company know whether an intruder has penetrated the firewall? Also, how can a company detect whether unauthorized employees are accessing restricted applications? **Intrusion-detection systems** monitor networks and application **log files** (files containing information on files, including who accessed them and when). If an intruder accesses either the network or an unauthorized application, the system detects the intrusion, halts the session and sets off an alarm to notify the system administrator.

38.7 Legal Issues

The Internet has posed significant challenges to the legal system of the United States. For example, file-sharing technology enables widespread copyright infringement, while Web-site personalization mechanisms threaten consumers' privacy. In this section, we investigate the legal differences between our physical environment, which consists of temporal and geographic boundaries, and **cyberspace**, the realm of digital transmission not limited by geography. We also explore such issues as defamation, copyright and pornography as they relate to the Internet.

38.7.1 Privacy

Although an individual's right to privacy is not explicitly guaranteed by the United States Constitution, protection from government intrusion is implicitly guaranteed by the First, Fourth, Ninth and Fourteenth Amendments.[41] The Fourth Amendment provides U.S. citizens with the greatest assurance of privacy, protecting them from illegal search and seizure by the government:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Many Internet companies collect personal information from users as they navigate through a site. While privacy advocates argue that such efforts violate individuals' privacy rights, online marketers and advertisers disagree, suggesting that the recording of user behavior and preferences helps online companies to better serve their customers. For example, if a user visits an online travel site and purchases a ticket from Boston to Philadelphia, the travel site might record this transaction. In the future, when a ticket goes on sale for the same flight, the Web site can notify the user.

Online privacy also affects companies' relationships with employees. Many businesses are implementing systems that regulate employee efficiency in the workplace. One of the newest surveillance technologies, **keystroke cops**, monitors employee activities on corporate and communications equipment.[42] Keystroke software is loaded onto the hard drive of an employee's computer, or it can be sent to an unsuspecting employee as an e-mail attachment. Once activated, the software registers each keystroke before it appears on the screen. In the debate about monitoring technology, the right of a business to regulate the use of company time and equipment is pitted against the employees' rights to privacy and freedom of speech. Situations can involve employees who neglect responsibilities to write personal e-mails, surf the Web or conduct online tirades against management in chat rooms.

38.7.2 Defamation

Defamation is the act of injuring another person's reputation, honor or good name through false written or oral communication.[43] It is often difficult to win a defamation suit because the First Amendment strongly protects the freedom of **anonymous speech** (speech by an unknown person or a person whose identity has been withheld).

Defamation consists of **slander** and **libel**. Slander is spoken defamation, whereas libelous statements are written or spoken in a context in which they have longevity and per-

vasiveness that exceed slander. For example, broadcast statements can be considered libelous, even though they are spoken.

To prove defamation, a **plaintiff** (the person bringing the case to court) must meet five requirements: (1) The statement must have been published, spoken or broadcast; (2) there must be identification of the individual(s) by name or reasonable association; (3) the statement must, in fact, be defamatory; (4) there must be fault (for public figures, the statement must have been made with **actual malice**, or with the intention of causing harm; for private persons, the statement needs only to have been **negligent**, or published, spoken or broadcast when known to be false); and (5) there must be evidence of injury or **actual loss.**[44]

38.7.3 Sexually Explicit Speech

Although pornography is protected under the First Amendment, obscenity is not, and parties can be held legally responsible for obscene statements. As determined in *Miller v. California* (1973), the **Miller Test** identifies the criteria used to distinguish between obscenity and pornography. To be determined obscene by the Miller Test, material must (1) appeal to the prurient interest, according to contemporary community standards, and (2) when taken as a whole, lack serious literary, artistic, political or scientific value.[45]

The Internet, with its lack of geographic boundaries, challenges the Miller Test. As we have stated, the test is dependent on contemporary community standards. In cyberspace, communities exist independently of physical locations. Cyberspace complicates issues of jurisdiction by making it possible, for example, for a person in Tennessee, where the tolerance for pornography is relatively low, to view a site that is hosted in California, where the tolerance is high.

The Internet possesses characteristics similar to those of broadcast media and print media, but problems arise in applying laws developed for those media to the Internet. Broadcasting is considered highly pervasive, and its content is strictly regulated. The Internet resembles broadcasting in its ability to reach a broad audience with little or no warning.[46] By contrast, the regulation of print media focuses on limiting the audience, rather than the content, of the material. Defined as **non-content-related means** (an effort to control the audience rather than the material), print restrictions, for example, allow an adult to purchase and view pornographic material, but limit an adolescent's ability to obtain the same material. The Internet can mimic non-content-related means by requiring users to provide identification before entering specific sites. Regulation of Web content could require the development of new legislation because of the Internet's unique features.

38.7.4 SPAM

E-mail marketing has taken on a new extreme as more and more people communicate through the e-mail and the Web. Spamming, as defined earlier, is sending mass e-mails to people who have not expressed interest in receiving such e-mails. Today, a typical Internet user or e-mailer may receive hundreds of spam e-mails per day.

Many people are working to construct legislation that puts an end to these unsolicited e-mails. Spam has many privacy concerns based not only on the sheer volume of e-mail sent per day but also the content of the e-mails. Consumers and businesses alike are affected by the decrease in e-mail server productivity due to the mass e-mails received. It is estimated that U.S. corporations alone lose $10 billion each year in lost productivity and com-

puting resources due to spam.[47] In addition, the graphic content sometimes advertised in these e-mails is unsuitable for some audiences, such as children.

IT departments and software companies are working to develop better software products that filter out or block readers from receiving spam in their inboxes. Typically the software searches for known spam keywords or products and prevents those e-mails from getting to the reader, but lots of spam messages still get through. Spam e-mailers keep reformatting their e-mails and e-mail addresses to attempt to stay one step ahead of the technology by changing their e-mail addresses every day and disguising the content with relevant material to make the e-mail appear normal. Spam will continue to be one of the toughest privacy and security issues that Internet users face as the growth of the Web continues.

38.7.5 Copyright and Patents

Copyright is the protection given to the author of an original work, including "literary, dramatic, musical, artistic and certain other intellectual works," whether the work has been published or not. For example, copyright protection is provided for literature, music, sculpture and architecture. Copyright protects only the expression or form of an idea, not the idea itself.

Copyright protection provides incentive to the creators of original material by guaranteeing them ownership of their work for a given time. Currently, copyright protection is guaranteed for the life of the author plus 70 years. Concerns have been raised regarding the ability of traditional law to protect intellectual-property owners from online copyright infringement because of the ease with which material can be reproduced on the Internet. To complicate the issue further, **digital copies** are perfect duplicates of digital originals, making it difficult to differentiate authorized copies from pirated ones.

One of the most heavily debated areas of copyright infringement and protection lies in the sharing and distribution of music files (MP3s) and movies over the Internet. The most widely recognized example of file-sharing software was Napster. Hundreds of thousands of people shared millions of music downloads with one other on a regular basis, all for free, without record companies or recording artists receiving a payment for their copyrighted material. The music industry took Napster to court, where they won a ruling which forced Napster to temporarily cease operations and required that if Napster were to continue its file-sharing software operations, it had to charge monetary fees for file downloads. While Napster is no longer a free service, several other file-sharing software distributors have emerged in its place, including Kaaza, Grokster, and Gnutella.[48]

The ability of Web users to obtain copyrighted material without paying proper compensation to the owners of the material in return is a big concern not only for the recording industry, but for other industries, such as publishing and film-making. If anyone can download "pirated" files without paying for them, then millions if not billions of dollars in potential revenue are lost each year for these companies and the products they create.

e-Fact 38.4

Analysts estimate that approximately 2.6 billion files per month are downloaded illegally from the Internet.[49]

Patents, another form of intellectual property, grant the creator sole rights to a new discovery. Given the growth rate of the Internet, some argue that the 17–20-year duration of patents discourages continuous software development and improvement.

In 1998, the federal regulations governing the distribution of patents increased the scope of patentable discoveries to include "methods of doing business."[50] To be granted a patent for a method of doing business, one must present an idea that is new, useful and not obvious to a skilled person.[51]

38.8 XML and e-Commerce

XHTML (see Chapters 4 and 5) is a markup language used for publishing information on the Web. Content developers use a fixed set of XHTML tags to describe the elements of online documents, such as headers, paragraphs, boldface text and italicized text.

Extensible Markup Language (**XML**), discussed in depth in Chapter 20, is similar to XHTML but has some distinguishing differences. With XML a used is allowed to create customized tags that are unique to specific applications and thus is not limited to XHTML's fixed set of publishing-industry-specific tags. For example, developers can make industry-specific (or even organization-specific) tags to categorize data more effectively within their communities. Some industries have already developed standardized XML tags for online document publication. For example, Mathematical Markup Language (MathML) is a standardized XML-based language for the marking up of mathematical formulas in documents, whereas Chemical Markup Language (CML) is a standardized XML-based language for the marking up of the molecular structure of chemicals.

The ability to customize tags enables business data to be used worldwide. For example, businesses can create XML tags specifically for invoices, electronic funds transfers, purchase orders and other business transactions. However, to be used effectively, an industry's customized tags must be standardized across the industry.

Once tags are standardized, the browser must be able to recognize them. This is accomplished by building the tags into the browser or by downloading the appropriate plug-ins. The process can be automated, because customized XML tags could actually be used as a command for a browser to download the plug-in for the corresponding set of standardized tags.

The impact of XML on e-commerce and Web services (discussed in Chapter 20) is profound. XML gives online merchants a superior method of tracking product information. By using standardized tags for data, bots and search engines are able to find products online more quickly.

Many industries are using XML to improve Electronic Data Interchange (EDI), the transfer of data between computers. The health care industry, for example, uses XML to share patient information (even CAT-scans) among health care applications. This helps doctors access information and make decisions more quickly, which can improve patient care.[52]

The **Health Level Seven** (**HL7**) organization's **Application Protocol for Electronic Data Exchange in Healthcare Environments** uses XML. This standard enables health care applications to exchange data electronically by specifying the layout and order of information. Patient names, addresses and insurance providers are tagged so that such data can be shared electronically among applications. For example, once a patient's identification information is entered, it can be shared over the hospital's intranet with the labs and the accounting department, eliminating the need to re-enter the same data. HL7 is a member of the non-profit **American National Standards Institute** (**ANSI**)—an accredited standards developing organization—that focuses on clinical and administrative data. To locate additional information on HL7, visit its Web site at `www.HL7.org`; the ANSI Web site is `www.ansi.org`.

The XML **Metadata Interchange Format** (**XMI**) is a standard that combines XML with the **Unified Modeling Language** (**UML**). Software developers use UML to design object-oriented systems. XMI allows developers using object technology to tag design data. XMI tags allow developers to exchange design data over the Internet and interact with multiple vendors by using a variety of tools and applications. XMI thus enables people worldwide to collaborate on the design of object-oriented software systems. For more information about XML and XMI, visit `www-106.ibm.com/developersworks/xml`.

Some software companies sell their products over the Web. The **Open Software Description Format** (**OSD**) is an XML specification that facilitates the distribution of software over the Internet. Using OSD, developers tag the structure of an application and its files. The tags describe each component of the software and its relationship to the other components in the application. The availability of software for download from the Web saves vendors the time, resources and money previously required to create boxed products and ship them to customers.

38.9 Introduction to Wireless Technology and m-Business

Wireless technology has developed into one of today's hottest topics because of its ability to bring the power of communications and the Internet into the hands of users worldwide. The introduction of wireless communications affects many aspects of society, including business management and operations, employee productivity, consumer purchasing behavior, marketing strategies and personal communications. As the popularity of wireless services grows, manufacturers are enabling wireless devices with an increasing array of features and capabilities. For example, many personal digital assistants (PDAs) now operate as cell phones, and vice versa.

38.10 m-Business

M-business, or **mobile business**, defined as e-business enabled by wireless communications, is one of the newest frontiers in electronic communications. While still in its initial stages, m-business promises rapid growth. This will be fueled by the ability of m-business to reach users effectively and allow them instant access to business-critical information and communications capabilities at any time, from almost anywhere.

Wireless access benefits businesses, employers, employees and consumers. For employers and employees, wireless access provides the ability to communicate, access corporate databases, manage administrative tasks (e.g., answer e-mail, schedule meetings) and enhance customer relations. In addition, wireless communications enables the streamlining of product shipment and tracking. Furthermore, both employees and consumers can manage responsibilities and complete tasks during idle time—waiting for a bus, or standing in line at a bank.

38.11 Identifying User Location

Location-identification technologies allow businesses and individuals to determine wireless users' locations to within yards. Some of the most impressive m-business applications are location-based services, or applications that are supported by location-identification technologies. Location-based services can be used to improve wireless marketing, customer

relationship management (CRM) and business-to-consumer (B2C) and business-to-employee (B2E) applications. For instance, if a business knows that a customer is near one of its stores or offices, the business could send notification of a sale or promotion to the user's handheld device. Emergency services and wireless accessibility also can be improved through the adoption of location-identification technologies. In this section, we introduce location-based services and their enabling technologies. We also examine the E911 Act, a government mandate that requires all cell phones to host location-identification technologies.

Location-based services are made possible by relationships among cellular service providers, cellular networks and mobile-device users. Many leading wireless companies have developed their own methods of determining a user's location. Some considerations that affect these methods are bandwidth availability, communication speed and **multipath errors** (errors resulting from signals reflecting off objects like buildings and mountains).

38.11.1 E911 Act

The **E911 Act** (the "E" stands for "Enhanced"), proposed by the Federal Trade Commission (FTC) in 1996 and signed into law in 1999, is designed to standardize and enhance 911 service across mobile devices. Its goal is to improve emergency response time to 911 calls made by cell-phone users. In addition, the **Disabilities Issues Task Force** of the FCC is making efforts to ensure that hearing- and speech-impaired people have access to 911 service through mobile devices. Although the E911 Act will improve the efficiency of emergency services, it raises concerns about the privacy of wireless users. Privacy issues in relation to wireless communications are discussed in Section 23.6.

The first phase of the E911 Act requires all wireless services companies to provide **Automatic Number Information** (**ANI**), or the phone numbers of cell phones calling in 911 emergencies. Carriers (e.g., AT&T, Verizon or Cingular) must also provide the locations of the **cell sites** (a cell site identifies the coverage area of a tower that receives and transmits cell-phone signals) receiving the 911 calls. Emergency technicians can use this information to determine users' locations, although only to within the range of the nearest tower. The second phase of the bill mandates that all mobile-phone carriers provide Automatic Location Identification (ALI) of a caller to within 125 meters, 67% of the time.

There are several benefits to the E911 Act. In many emergency situations, drivers do not know their exact locations. Information provided by the new technology can help emergency-response teams accurately locate callers, improve response times and reduce the consequences of injuries. In addition, if a call breaks up or the operator cannot understand the caller, emergency personnel can obtain the information necessary to find and assist the caller.[53]

38.11.2 Location-Identification Technologies

Location-identification technologies enable businesses to provide wireless users with location-based services. For example, when a user asks for directions to the nearest coffee shop, the wireless carrier can use **triangulation** to determine the location of the user's wireless device. Triangulation is a popular technique employed by many location-identification technologies. A user's location is determined by analyzing the angles of cell-phone signals from (at least) two fixed points a known distance apart. This information is presented to the **content provider** (the business offering the location-based service) in the form of a **geocode** (the latitude and longitude of the user's location). The geocode is then translated into

a map or step-by-step navigational instructions with the help of a mapping service, and this information is passed to the user. Figure 38.6 outlines various location-identification technologies and their accuracy levels.

Technology	Degree of Accuracy
Cell of Origin (COO)	Least accurate. User could be anywhere in tower's range. Meets only Phase I of E911 Act.
Angle of Arrival (AOA)	Fairly accurate. User is within the overlap of two towers' cell sites. Used primarily in rural areas where there are fewer towers. Complies with Phase II of E911.
Time Difference of Arrival (TDOA)	Accurate. User's location is determined by triangulating from three locations. Complies with Phase II of E911. Most effective when towers are close together.
Enhanced Observed Time Difference (E-OTD)	Accurate. User's location is determined by triangulating from three locations. Complies with Phase II of E911.
Location Pattern Matching	Accurate. User's location is determined by analyzing multipath interference in a given area, making the method more effective for locating a device in an urban area.
Global Positioning Systems (GPS)	Highly accurate. Satellites determine a user's location anywhere on earth. Not as effective when the user is indoors.

Fig. 38.6 Location-identification technologies.

38.12 Wireless Marketing, Advertising and Promotions

Wireless communications, the Internet and the World Wide Web provide marketers with new tools for the development and delivery of marketing campaigns. Wireless technologies in particular have greatly enhanced the ability of organizations to target consumers and provide timely, relevant content. In this section, we discuss marketing via wireless devices and the delivery of wireless promotions and advertising. We also introduce aspects of customer relationship management via wireless communications.

E-marketing and m-marketing should be used in conjunction with traditional marketing to create an effective corporate marketing strategy. This strategy should focus on attracting new customers and repeatedly bringing them back. Because wireless marketing requires the alteration of traditional marketing strategies to meet the demands of wireless devices and consumers, marketers should develop wireless sites and campaigns separately from, but in parallel with, online initiatives. E-marketing is discussed earlier in this chapter (see Section 38.4).

Wireless marketing can be classified as a **pull strategy**, a **push strategy** or a combination of both.[54] A pull strategy assumes that users will request that specific information be sent to their wireless devices in real time. By contrast, a push strategy is enacted when an organization delivers marketing messages to wireless devices at a time deemed appropriate by the company, rather than in real time. Regardless of which strategy is used, wireless marketing should be permission-based, also known as **opt-in**. **Permission-based**

marketing protects customers' privacy and provides a well-defined target market, increasing campaign response rates and productivity. By allowing users to control the number and type of messages they receive, marketers can improve customer satisfaction and campaign results. In addition, an opt-in policy can decrease the costs associated with wireless campaigns, because marketing material is delivered only to consumers who have expressed interest in the company and its products or services.

Successful implementation of wireless advertising requires that the content provider, advertiser and carrier establish a system that delivers ads to consumers at the right location and the right time. When combined with location-identification technologies and location-based services, wireless advertising offers the benefit of highly targeted information delivery. For example, an individual who receives an e-coupon from a nearby fast-food restaurant is far more likely to respond to the ad than a consumer 50 miles away who is sent a coupon for the same restaurant. The ability to provide location-specific advertisements increases the value of the advertisements, as companies are willing to pay more for ads to which many customers respond.

Although wireless communications provide many benefits, they also create new obstacles for advertisers. Security issues arise, because content delivered over the wireless Internet may be vulnerable at certain points during transmission. Security is discussed in detail earlier in this chapter (see section 38.6). Marketers must ensure that messages appear in the intended format. Limited technology and multiple protocols cause content to be displayed differently on various receiving devices. In addition, cell-phone reception is poor in some areas, and service can disconnect while customers are ordering or inquiring about a product or service.[55] Wireless advertising is further hindered by the lack of wireless-advertising standards and the complex value chain that exists in the wireless-advertising industry. Traditionally, advertisers work with publishers, who deliver advertisements to consumers through various media. When advertisements are distributed to wireless devices, a wireless carrier is added to the chain, as publishers must go through carriers to reach consumers. It is usually the **carrier** that captures users' geographic locations. Carriers have the potential to control the type and amount of wireless advertising that reaches their subscribers. It can be difficult to convince carriers to allow advertising through their services because the carriers do not want to annoy their customers.

To reach wireless customers, advertisers must either develop an in-house solution or use a wireless ad-serving network to deliver ads. A **publisher** or **publisher network** (i.e., a site or group of sites that carry wireless content and wireless advertisements) must also be selected. Advertisers should evaluate carriers' and publishers' wireless-transmission protocols; a device that operates on one standard may not be able to receive an advertisement designed for a different standard, and advertisers should work with carriers and publishers to minimize such problems. For example, sometimes graphics are more effective than text in a wireless advertisement, because graphics can display a font smaller than those supported by the device. Using a graphic, the advertiser may be able to send more text than is possible in a text-formatted ad. However, marketers must be aware that some wireless devices cannot display graphics.[56]

Short Message Service (**SMS**), a service that delivers text messages of up to 160 alphanumeric characters, is one option for delivering wireless advertisements. When marketers send SMS messages, the length, creativity and interactivity of the message are limited because the message cannot contain graphics. However, text messages take far less

time to load than rich multimedia and graphics-packed messages.[57] SMS can also be used to send mobile alerts, which provide customers with valuable news and product updates.[58]

m-Fact 38.1

Over 12 billion messages per month are sent through SMS worldwide.

Alternatively, companies can send promotions to customers by distributing e-coupons to their wireless devices. For example, wireless promotions delivered to automobile drivers and passengers can alert them to nearby shopping malls, gas stations and restaurants that are offering special deals. However, some users might find this kind of advertising intrusive. A wireless promotional strategy can enable opt-in users to indicate the type and amount of promotional information they wish to receive, and to select the time of day that the coupons will be sent.

Wireless communications also can be used to improve customer relationship management (CRM). CRM focuses on providing and maintaining quality service for customers by effectively communicating and delivering products, services, information and solutions. By using wireless devices, customers can receive timely and relevant information on demand, and companies can interact more efficiently with their sales and field forces.

Sales-force automation assists companies with aspects of the sales process, including the maintenance and discovery of leads and the management of contacts. Sales-force automation can lighten the administrative load on the sales force, allowing salespersons to focus on important details and leads that can increase revenue. Furthermore, information about products and customers can be accessed in real time, providing salespeople with current company and client information.[59]

A sales force's ability to access information almost anywhere at any time improves its level of overall production. For example, imagine that a salesperson is at a professional hockey game with a client. The client asks the salesperson a question that must be answered before the sale can be made. Using a cell phone or PDA, the salesperson can access information at that moment and close the sale. Without the wireless Internet and enabled devices, the salesperson would have had to call the office or find a wired Internet connection—which is not easy to do at a sporting event.

38.13 Wireless Payment Options

Secure electronic funds transfer and positive user transaction experiences are crucial to the success of e-commerce and m-commerce. Businesses that offer domestic and international products and services must ensure that **m-payments** (payments made via wireless devices) will be received securely and that the transactions are valid.

The variety of wireless devices, the lack of m-payment **interoperability** and the immaturity of the m-payment industry have led to inconsistent user experiences. Interoperability, the ability for transactions to be performed using any software or device, is a major hurdle for the m-payment market. Organizations such as the **Global Mobile Commerce Interoperability Group** (**GMCIG**) and the **Mobile Electronic Transactions** (**MeT**) **Group** support standards that enhance interoperability.

Traditionally, banks and credit-card companies process payments. Currently, micropayments, discussed earlier in this chapter (see Section 38.5.3), are the most popular m-payment application. This creates problems, because banks and credit-card companies

cannot process micropayments profitably. Often, the cost to financial institutions of processing small payments is more than the actual payment amount. Mobile-phone operators are best suited to handle micropayments because the phone bills that they produce are composed almost exclusively of small charges. However, mobile operators are not equipped to assume the financial risk associated with payment processing for services other than theirs, and consumers may not trust a mobile operator to act as a financial institution.[60]

To address this issue until m-payments are used for larger purchases, banks and wireless operators have begun to form partnerships. Through such affiliations, wireless operators can offer their users a convenient billing system for m-payments, while banks provide experience in payment processing and financial risk management. Another alternative is for banks to become **Mobile Virtual Network Operators** (**MVNO**). MVNOs purchase bandwidth capacity from mobile carriers and resell it under their brand name, coupled with value-added services.[61]

M-wallets (similar to the e-wallets discussed earlier in this chapter; see Section 38.5.2) are the most common form of transaction software offered by the developing m-payments market. M-wallets, like e-wallets, allow users to store billing and shipping information. Users can recall this information and enter it with one click while shopping from a mobile device. Data entry on wireless devices can be time-consuming, because most devices have small keypads on which multiple keys must be pressed to display a correct letter. By enabling one-click shopping, m-wallet software simplifies the ordering process and adds convenience to m-business transactions. In addition, companies are integrating new technologies into m-wallet software. For example, some products use speech-recognition and voice-authentication technologies to enable cell-phone users to make purchases by speaking into their phones. Such applications eliminate the need for keypad data entry.[62]

38.14 Privacy and the Wireless Internet

As we discussed earlier in this chapter (see Section 38.7.1), the Internet presents many new consumer privacy issues. When people communicate through wireless devices, privacy is further threatened; transmissions can be intercepted, and users can be located with a high degree of accuracy. Wireless location tracking will offer access to information about users' activities, including where they go, when they go and the length of their stay. Over time, a compilation of this data could contribute to a substantial profile of a user's habits.

Currently, the accepted protocol for collecting a user's information is an opt-in policy. In some cases, a business installs a **double opt-in** policy. Double opt-in policies require the user to request information and then to confirm the request by replying to a follow-up e-mail. In theory, this practice provides greater protection of privacy. An **opt-out** policy enables an organization to send marketing information to consumers until they request to be removed from the mailing list.

When an opt-in policy is used, consumers request and expect the information that they receive from advertisers. Companies that wish to collect personal information must tell consumers how their information will be managed. The complicated legalese of privacy policies is difficult to display effectively on small interfaces, making the wireless Internet more susceptible to privacy violations. For example, if a company has partners or affiliates, location information might be shared with and used by these companies. As a result, consumers could find themselves bombarded with unsolicited e-mail while they are in their cars, at the movie theater or enjoying an evening out. In addition, although the Federal Communications Com-

mission (FCC) has guidelines outlining a telecommunications carrier's responsibilities for protecting user privacy, marketers and vendors are not subject to the same guidelines.[63] Third-party vendors, in most cases, will have their own privacy policies.

To date, there is no legislation that monitors the use and misuse of location-identification technology. Industry leaders and government agencies fear that such legislation could slow the development of wireless technology. Even if the government perceives a need for regulation, there are many ways to approach privacy legislation; one "comprehensive" privacy law could target some issues but miss others. Personal information collected from wireless users, for example, can be of a different nature than that collected from wired users.

To address privacy concerns, the **Cellular Telecommunications and Internet Association (CTIA)** has issued a set of guidelines for protecting consumer privacy. These include: (1) companies should alert consumers when their locations are being identified, (2) opt-in should be the standard, meaning that companies should inform users of the services that they will receive in exchange for personal information and allow them to make educated decisions, (3) consumers should be able to access their own information and (4) the same protections should be offered to all consumers, regardless of carrier or device.[64]

38.15 Web Resources

Storefront Model

`www.barnesandnoble.com`
One of the first brick-and-mortar companies to make a large-scale commitment to the Web, Barnes & Noble sells books, e-books, CDs and software on its Web site, using shopping-cart technology.

`www.Moviefone.com`
Moviefone enhances its offline efforts by allowing people to buy advance tickets to movies from its Web site. Visitors can also view movie trailers, read cast interviews and get the latest movie reviews.

Auction Model

`www.eBay.com`
This is the best-known and most successful auction site on the Web.

`www.auctiontalk.com`
This site is an auction portal, providing links to other auctions and specific products being auctioned at various sites online.

Portal Model

`www.google.com`
Google is an advanced search engine that ranks search results by the true popularity of the Web site. The more people that follow a link to a site, the higher the site will appear in a search.

`www.yahoo.com`
Yahoo! is a portal allowing people to search the Web using a traditional search engine, Yahoo! also offers games, e-business solutions and free e-mail.

Name-Your-Price Model

`www.priceline.com`
The originator and patent holder of the name-your-price model, `Priceline.com` gives customers the ability to name their price for travel arrangements and scores of other products and services.

`www.ticketsnow.com`
Finding low-priced tickets to concerts and the theater is often difficult. This site allows people to bid for a lower price on their tickets.

Comparison-Pricing Model

`www.froogle.com`
Froogle uses the search-engine technology to compare product and service pricing and post the results to the user ranked by relevancy.

`www.pricewatch.com`
People interested in building a computer or upgrading their current system will find the lowest prices on computer equipment on this price-comparison Web site.

Bartering Model

`www.itex.com`
This site facilitates B2B transactions by allowing members to trade assets through the `itex.com` Web site.

Free Turnkey Solutions

`www.websiteforfree.com`
The free portion of the site's services include home-page design, the ability to make site corrections and use of the site's educational resources.

`www.freemerchant.com`
This site provides a free turnkey solution for building an online store and offers hosting, store-building capabilities and a shopping-cart model at no cost to the user.

Credit-Card Payment

`www.cybercash.com`
CyberCash (now owned by Verisign) enables e-merchants to accept credit-card payments online. The company also offers an e-wallet technology and an online bill-paying service.

`www.trintech.com`
Trintech offers a secure credit-card payment system that enables simultaneous purchases from multiple stores. This is used in virtual shopping malls.

E-Wallets

`www.visa.com/pd/ewallet/main.html`
Visa offers various e-wallets for use with Visa credit cards. These wallets are backed by the financial institution that issues the Visa card.

Checking Account Payment

`www.debit-it.com`
This site allows merchants to draw against the balances in their checking accounts as a valid form of payment over the Internet.

Digital Cash

`www.ecash.net`
eCash offers digital-cash services for both online purchases and peer-to-peer payments.

`www.paypal.com`
Paypal is a payment solution that allows customers to establish an account with all necessary purchasing information, then use that account to conduct business over the Web without having to enter personal information time and time again. Similar to an online bank account or credit card.

Smart Cards

`www.visa.com/nt/chip/info.html`
This page contains information on a smart card being offered by Visa, which will contain a digital-cash application and e-wallet services.

`www.americanexpress.com`
American Express offers the Blue smart card (personal and corporate) and related services through its Web site.

Micropayments

`www.hut.fi/~jkytojok/micropayments`
This is a paper on electronic-payment systems with a focus on micropayments.

`www.echarge.com`
eCharge partners with AT&T to provide micropayment services billed to the user's phone bill.

Online Privacy

`www.cdt.org`
The Center for Democracy and Technology has expertise in the legal and technological development of the Web. Its mission is to protect privacy and free speech.

`www.eff.org`
The Electronic Frontier Foundation is a nonprofit organization concerned with privacy and freedom of expression in the digital age.

Search-Engine Information

`www.webdeveloper.com/html/html_metatags.html`
Web Developer provides a tutorial on meta tags.

General Internet Marketing Information

`www.eMarketer.com`
eMarketer aggregates content on Internet marketing, including news, statistics, profiles and reviews.

`www.channelseven.com`
Channel Seven is a news and information site that helps marketing and advertising professionals keep up-to-date with the Web.

Complete CRM Solutions

`www.peoplesoft.com`
PeopleSoft® created the *Vantive Enterprise* and the *Web-based Vantive eBusiness application suites* to fulfill companies' customer relationship management needs. The modules of the solution can be used separately or together and include *Vantive Quality, Vantive Support, Vantive Sales, Vantive Field Service* and *Vantive HelpDesk*.

`www.pegasystems.com`
Pegasystem offers a full range of CRM solutions for service, marketing and sales, using various channels of contact with consumers.

Security Resource Sites

`www.securitysearch.net`
This is a comprehensive resource for computer security. The site has thousands of links to products, security companies, tools and more. The site also offers a free weekly newsletter with information about vulnerabilities.

theory.lcs.mit.edu/~rivest/crypto-security.html
The Ronald L. Rivest: Cryptography and Security site has an extensive list of links to security resources, including newsgroups, government agencies, FAQs, tutorials and more.

Government Sites for Computer Security

www.usdoj.gov/criminal/cybercrime/compcrime.html
Visit this site for information about the U.S. government's efforts against cybercrime and to read about recently prosecuted cases.

cs-www.ncsl.nist.gov
The Computer Security Resource Clearing House is a resource for network administrators and others concerned with security. This site has links to incident-reporting centers, information about security standards, events, publications and other resources.

Internet Security Vendors

www.rsasecurity.com
RSA is one of the leaders in electronic security. Visit this site for more information about its current products and tools, which are used by companies worldwide.

www.ca.com
Computer Associates is a vendor of Internet security software. It has various software packages to help companies set up a firewall, scan files for viruses and protect against viruses.

Public-Key Cryptography

www.entrust.com
Entrust produces effective security software products using Public Key Infrastructure (PKI).

www.cse.dnd.ca
The Communication Security Establishment has a short tutorial on Public Key Infrastructure (PKI) that defines PKI, public-key cryptography and digital signatures.

Digital Signatures

www.ietf.org/html.charters/xmldsig-charter.html
The XML Digital Signatures site was created by a group working to develop digital signatures using XML. You can view the group's goals and drafts of its work.

www.elock.com
E-Lock Technologies is a vendor of digital-signature products used in public key Infrastructure. This site has an FAQs list covering cryptography, keys, certificates and signatures.

Digital Certificates

www.verisign.com
VeriSign creates digital IDs for individuals, small businesses and large corporations. Check out its Web site for product information, news and downloads.

www.silanis.com
Silanis Technology is a vendor of digital-certificate software.

SSL

www.netscape.com/security/index.html
The Netscape Security Center is an extensive resource for Internet and Web security. You will find news, tutorials, products and services on this site.

www.openssl.org
The Open SSL Project provides a free open-source toolkit for SSL.

Firewalls

`www.interhack.net/pubs/fwfaq`
This site provides a list of FAQs on firewalls.

`www.thegild.com/firewall`
The Firewall Product Overview site has an extensive list of firewall products, with links to each vendor's site.

IPSec and VPNs

`www.ietf.org/html.charters/ipsec-charter.html`
The IPSec Working Group of the Internet Engineering Task Force (IETF) is a resource for technical information related to the IPSec protocol.

`www.ip-sec.com`
The IPSec Developers Forum allows vendors and users to test the interoperability of different IPSec products. The site includes technical documents related to the IPSec protocol.

Wireless Security

`www.radicchio.cc`
Radicchio is a nonprofit organization dedicated to the development and promotion of standards and technologies for secure mobile business.

Location-Based Service Providers

`www.trueposition.com`
TruePosition® uses TDOA technology to provide location-based services. TruePosition specializes in E911 applications.

`www.ericsson.com`
GSM phones can be located by using the *Ericsson Mobile Positioning System*. Ericsson has developed a wide variety of wireless-location solutions.

Location-Based Technology News and Information

`www.lbszone.com`
This site provides links to news regarding location-based services and leading location-based service providers.

Location-Based Services Standards and Legislation

`www.locationforum.org`
The Location Interoperability Forum (LIF) is dedicated to developing standards for location-identifying technologies.

`www.fcc.gov/e911/enhanced`
This Web site was established by the FCC to provide information regarding the E911 Act.

`www.fcc.gov/Bureaus/Wireless/Public_Notices/2000/da002099.html`
This Web site was established by the FCC to provide details about the automatic location-identification specifications of the E911 Act.

Wireless Marketing and Advertising

`www.mobliss.com`
Mobliss develops wireless marketing solutions and focuses on targeting and tracking campaigns, including games, contests, sweepstakes and location-based promotions.

`www.digitalimpact.com`
Digital Impact designs and implements direct permission-based marketing campaigns. The company tracks and analyzes campaign results and delivers marketing through online and wireless channels.

`www.advertising.com`
This company provides marketing solutions for the Web, e-mail and wireless platforms. Ads are served for PDAs, on wireless Internet sites and through SMS.

SUMMARY

- E-commerce involves exchanges among customers, business partners and vendors. E-business is composed of these same elements, but also includes operations that are handled within the business itself.
- The transition from brick-and-mortar businesses to click-and-mortar businesses is happening in all sectors of the economy.
- The banking industry uses Electronic Funds Transfer (EFT) to transfer money between accounts.
- Electronic Data Interchange (EDI) standardizes business forms, such as purchase orders and invoices, so that companies can share information electronically with customers, vendors and business partners.
- The storefront model combines transaction processing, security, online payment and information storage to enable merchants to sell their products online.
- Shopping-cart technology allows customers to accumulate items they wish to buy. A widely recognized example of an e-business that uses shopping-cart technology is `Amazon.com`.
- Auction sites allow users to pinpoint the lowest prices on available items.
- The reverse-auction model allows the buyer to set a price that sellers compete to match or even beat. A reserve price is the lowest price that the seller will accept.
- Portal sites give visitors the chance to find what they are looking for in one place. Search engines are horizontal portals, or portals that aggregate information on a broad range of topics. Vertical portals are more specific, offering information pertaining to a single area of interest.
- The name-your-price business model allows customers to state the price they are willing to pay for products and services.
- Intelligent agents are programs that search and arrange large amounts of data and report answers based on that data.
- The comparison-pricing model allows customers to poll a variety of merchants and find a desired product or service at the lowest price.
- The demand-sensitive-pricing business model follows the idea that the more people who buy a product in a single purchase, the lower the cost per person becomes.
- A popular method of conducting e-business is bartering, or offering one item in exchange for another.
- Some businesses establish an online presence by using a turnkey solution (a prepackaged e-business). Other options include e-business templates that outline the basic structure, but allow the design to be determined by the owner.
- Components of a marketing campaign include branding, e-mail, marketing research, advertising, promotions and public relations.
- A brand is a name, logo or symbol that helps identify a company's products or services.
- Spamming is mass e-mailing to people who have not expressed interest in receiving such e-mails. Spamming can give a company a poor reputation.

- While generating Web-site traffic is important to the success of an e-business, keeping user profiles, recording visits and analyzing promotional and advertising results are also helpful in measuring a marketing campaign's effectiveness.
- The target market is the group of people toward whom it is most profitable to aim a marketing campaign. Tracking devices, such as ID cards and cookies, are used to monitor consumer behavior.
- A search engine is a program that scans Web sites and lists relevant sites on the basis of keywords or other search-engine ranking criteria. Some search engines rank sites by sending out a program called a spider to inspect the site.
- An affiliate program is a form of partnership in which a merchant pays affiliates (other companies or individuals) for specified actions taken by visitors who click-through from an affiliate site to a merchant site.
- Promotions can attract visitors to a site and can influence purchasing.
- Public relations (PR) keeps customers and employees current on the latest information about products, services and internal and external issues, such as company promotions and consumer reactions.
- Customer relationship management (CRM) focuses on providing and maintaining quality service for customers.
- Digital cash is one example of digital currency. It is stored electronically and can be used to make online electronic payments.
- E-wallets keep track of billing and shipping information so that it can be entered with one click at participating merchants' sites.
- Smart cards are able to store more information than ordinary credit cards. Smart cards can require the user to have a password, giving the smart card a security advantage over credit cards.
- There are four fundamental requirements of a successful and secure transaction: privacy, integrity, authentication and nonrepudiation.
- Public-key cryptography uses two inversely related keys: a public key and a private key. The most commonly used public-key algorithm is RSA.
- The Secure Sockets Layer (SSL) protocol is commonly used to secure communication on the Internet and the Web. SSL uses public-key technology and digital certificates to authenticate the server in a transaction and to protect private information as it passes from one party to another over the Internet.
- Defamation is the act of injuring another's reputation, honor or good name through false written or oral communication. Defamation has of two forms, slander and libel. Slander is spoken defamation, whereas libelous statements are written or spoken in a context in which they have longevity and pervasiveness that exceed slander.
- The Miller Test identifies the criteria used to distinguish between obscenity and pornography.
- Copyright is the protection given to the author of an original work.
- Wireless technology has developed into one of today's hottest topics.
- The wireless medium affects business management and operations, employee productivity, consumer purchasing behavior, marketing strategies and personal communications.
- M-business is defined as e-business enabled by wireless communications.
- Businesses and individuals can determine wireless users' locations within yards by using location-based services.
- The E911 Act is designed to standardize and enhance 911 service across mobile devices. Phase 1 of the E911 Act requires all wireless cellular carriers to provide Automatic Number Information

(ANI), or the phone numbers of cell phones calling in 911 emergencies. The carriers must also provide the locations of the cell sites receiving the 911 calls (a cell site identifies a particular tower's area of coverage).

- Phase 2 of the E911 Act mandates that all mobile-phone carriers provide Automatic Location Identification (ALI) of a caller within 125 meters, 67% of the time.
- Triangulation determines a user's location by analyzing the angles from (at least) two fixed points a known distance apart.
- A geocode is the latitude and longitude of the user's location.
- A pull strategy assumes that people will request that specific information be sent to their wireless devices in real time. A push strategy is enacted when marketing messages requested by the recipient are not delivered to wireless devices in real time.
- Permission-based marketing helps guard customer privacy. It also increases campaign response rates and productivity, because the target market is better defined.
- Limited technology and a variety of protocols cause marketing content to be displayed differently on various receiving devices.
- The carrier determines the type and amount of wireless advertising that reach its subscribers.
- To reach wireless customers, advertisers must either develop an in-house solution or use a wireless ad-serving network to deliver ads.
- A publisher or publisher network is a site or group of sites that carry wireless content and wireless advertisements.
- Wireless advertisements can be delivered by using Short Message Service (SMS), a service that transmits text messages of 160 alphanumeric characters or less.
- Sales-force automation assists companies in the sales process, including the maintenance and discovery of leads and the management of contacts and other sales-force activities.
- The variety of wireless devices, the lack of m-payment interoperability and the immaturity of the m-payment industry have created inconsistent user experiences in relation to m-payment applications.
- Interoperability is the ability for transactions to be performed using any software or device.
- Mobile transactions are well suited for micropayments, which are payments under $10.
- Some banks are becoming Mobile Virtual Network Operators (MVNOs). MVNOs purchase bandwidth capacity from mobile carriers and resell it under their brand names, coupled with value-added services.
- M-wallets allow a user to store billing and shipping information that the user can recall with one click while shopping from a mobile device.
- The accepted protocol for collecting user information is called an opt-in policy—the user requests targeted information. An opt-out policy allows organizations to send information to consumers until they request to be taken off the mailing list.
- The Cellular Telecommunications and Internet Association (CTIA) has issued guidelines for protecting consumer privacy.
- Market penetration refers to the percentage of the population using a marketed service.
- Messaging is the ability to send brief text messages to the display of another cell phone.
- Extensible Markup Language (XML) allows users to create customized tags unique to specific applications. The ability to customize tags will allow business data to be used worldwide.
- The Open Software Description Format (OSD) is an XML specification that enables the distribution of software over the Internet.

TERMINOLOGY

actual loss
actual malice
affiliate program
affiliate site
anonymous speech
asymmetric keys
authentication
barter
bidder
brand
brand equity
brick-and-mortar business
business-to-business (B2B)
call handling
card-not-present (CNP)
certificate authority
certificate repositories
cipher
click-and-mortar business
click-through
client/server application
collision
comparison-pricing model
contact smart card
contactless smart card
contemporary community standards
cookie
copyright
cracker
crisis management
cryptography
cryptosystem
customer relationship management (CRM)
cyberspace
database
decryption key
defamation
demand-sensitive pricing
demographic
digital cash
digital certificate
digital copy
digital signature
digital wallet
direct e-mail
distributed denial-of-service
dynamic pricing
e-business
e-commerce
Electronic Data Interchange (EDI)
Electronic Funds Transfer (EFT)
electronic wallet
encipher
encryption
firewall
gateway
hacker
hash function
hash value
horizontal portal
ID card
integrity
intelligent agent
Internet mailing list
intrusion-detection system
IP address
IPSec (Internet Protocol Security)
key
key algorithm
keystroke cops
libel
local area network (LAN)
log file
log-file analysis
marketing mix
m-business
m-commerce
merchant account
merchant server
merchant site
message digest
message integrity
meta tag
Metadata Interchange Format (XMI)
method of doing business
micropayment
Miller Test
name-your-price model
negligent
noncontent-related means
nonrepudiation
online focus group
Open Software Description Format (OSD)
opt-in
packet
patent
peripheral component interconnection (PCI)
personalization

plaintext
point-of-sale (POS) transaction
point-to-point connection
portal
press release
privacy
private key
psychographics
public key
Public Key Infrastructure (PKI)
public relations
public-key algorithm
public-key cryptography
reach
reliability
reserve price
reverse auction
RSA
sales tracking
search engine
secondary research
secret key
secret-key cryptography
secure sockets layer (SSL)
seller
shopping bot
shopping cart
slander
smart card
smart-card reader
socket
spamming
spider
storefront
storefront model
supply chain management
symmetric cryptography
symmetric secret key
target market
TCP/IP
transaction support
turnkey solution
24/7
Unified Modeling Language (UML)
user profile
vertical portal
Virtual Private Network (VPN)
virus
Web bug
wireless application protocol (WAP)
wireless PKI (WPKI)
wireless transport layer security (WTLS)
worm

SELF-REVIEW EXERCISES

38.1 State whether each of the following is *true* or *false*. If *false*, explain why.

a) To conduct electronic commerce, a company must implement storefront technology.
b) Electronic Data Interchange (EDI) is the system that uses standardized electronic forms to facilitate transactions between businesses and their customers, suppliers and distributors.
c) In public-key technology, the same key is used to both encrypt and decrypt a message.
d) Secure Sockets Layer protects data stored on the merchant server.
e) Secure Electronic Transaction is another name for Secure Sockets Layer.
f) A shopping bot is a shopping cart that allows you to buy items from different stores, all at the same time.
g) XML allows developers to create unique tags to define specialized data.

38.2 Fill in the blanks in each of the following statements:

a) Customers are able to store products they wish to purchase in a(n) _____ while they continue to browse the online catalog.
b) Public-key encryption uses two types of keys, the _____ and the _____.
c) _____ learn more about a customer over time.
d) The type of cryptography in which the message sender and recipient both hold an identical key is called _____.
e) A customer can store purchase information and multiple credit cards in an electronic purchasing and storage device called a(n) _____.

ANSWERS TO SELF-REVIEW EXERCISES

38.1 a) False. Companies have many options when it comes to the design of their e-business. A storefront is a popular method, but it is not the only method. b) True. c) False. Separate, inversely related public and private keys are used. d) False. Secure Sockets Layer is an Internet security protocol that secures the transfer of information in electronic communication. It does not protect data stored on a merchant server. e) False. Secure Electronic Transaction is a security protocol designed by Visa and MasterCard as a more secure alternative to Secure Sockets Layer. f) False. A shopping bot can be used to search multiple Web sites for the best available prices and availability. g) True.

38.2 a) Shopping cart. b) Public key, private key. c) Intelligent agents. d) Secret-key encryption. e) Electronic wallet.

EXERCISES

38.3 State whether each of the following is *true* or *false*. If *false*, explain why.

a) A search engine pays companies for pre-specified actions taken by visitors who click through from an affiliate site.
b) CRM attracts visitors to a site and uses private-key encryption.
c) Smart cards can store more information than credit cards.
d) RSA is a method of preventing slander and libel on the Web.
e) The Open Software Description Format (OSD) allows software to be distributed over the Internet.

38.4 Fill in the blanks in each of the following statements:

a) _____ is stored electronically and can be used to make online electronic payments.
b) The _____ model allows customers to poll a variety of merchants and find a desired product or service at the lowest price.
c) The _____ model combines transaction processing, security, online payment and information storage to enable merchants to sell their products online.
d) The four fundamental requirements of a successful, secure transaction are: _____, _____, _____ and _____.
e) The _____ identifies the criteria used to distinguish between obscenity and pornography.

38.5 Define each of the following terms:

a) Cryptography.
b) Public key.
c) SSL
d) Auction.
e) Personalization.
f) E-wallet.
g) Shopping bot.
h) Intelligent agent.
i) Private key.
j) XML
k) Cookies.

38.6 Make a spreadsheet containing a column for each of the following business models: storefront model, auction model, name-your-price-model and B2B-exchange model. In each column, list three e-businesses that operate in the corresponding model. Visit the Web site of each of the companies you have selected. Answer the following questions:

a) Do the companies operate with more than one of the defined business models (e.g., storefront and auction)? If so, which models do they implement?

b) Are the companies Internet-only companies, or click-and-mortar businesses?
c) How do the companies generate revenue?

WORKS CITED

The notation <www.domain-name.com> indicates that the citation is for information found at that Web site.

1. A. Bartels, "The Difference Between E-Business and e-Commerce, "*Computerworld,* October 30, 2000, p. 41.

2. <www.info-edge.com/samples/EM-2080sam.pdf>

3. F. Hayes, "Masoned," *Computerworld,* May 17, 1999, p. 116.

4. L. Himelstein and R. Hof, "eBay vs. Amazon.com," *Business Week,* May 1999, p. 128.

5. D.K. Berman and H. Green, "Cliff-Hanger Christmas," *Business Week e.biz,* October 23, 2000, p. 33.

6. "Where the Auction Is—The B2B Market Hits $52 Billion in 2002," <www.iconocast.com> March 23, 2000.

7. <http://pages.ebay.com/community/aboutebay/overview/index.html>.

8. A. Salkever, "Will Froogle Be a Google for Shoppers?" <www.businessweek.com/technology/content/jan2003/tc20030114_5644.htm> 14 January 2003.

9. <http://froogle.google.com/froogle/about.html>.

10. <smallbusiness.yahoo.com/merchant>.

11. <www.yahoo.com>.

12. P. Seybold, "Broad Brand," *Industry Standard,* November 6, 2000, p. 214.

13. <www.dictionary.com/cgi-bin/dict.pl?term=psychographics>.

14. D. Greening, "When Push Comes to Shove," *Webtechniques,* April 2000, pp. 20, 22, 23.

15. D. Scott, "Paying Your Way to the Top," *eContent,* May 2003, pp. 33–38.

16. Q. Hardy, "All Eyes On Google," *Forbes,* May 26, 2003, pp. 100–110.

17. K. Hammonds, "Growth Search," *Fast Company,* April 2003, pp. 76–81.

18. B. Thompson, "Keeping Customers Is Smart and Profitable," *Business Week Special Advertising Section,* July 3, 2000.

19. <www.online-commerce.com/tutorial2.html>.

20. <www.paypal.com>.

21. M. Kane, "eBay Picks Up PayPal for 1.5 Billion," <http://news.com.com/2100-1017-941964.html> July 8, 2002.

22. S. Smith, "Paying for Content and Making Content Pay: Online Micropayment Strategies and Solutions," *eContent,* April 2003, pp. 26–30.

23. M. Solomon, "Micropayments," *Computerworld* 1 May 2000: 62.

24. "What's So Smart About Smart Cards?" *Smart Card Forum.*

25. <www.gemplus.com>.

26. B. Gates, "Bill Gates: Trustworthy Computing," 17 January 2002 <www.wired.com/news/business/0,1367,49826,00.html>.

27. <www.rsasecurity.com/rsalabs/rsa_algorithm>.

28. <www.pgpi.org/doc/overview>.

29. <www.rsasecurity.com/rsalabs/faq>.

30. S. Abbot, "The Debate for Secure E-Commerce," *Performance Computing,* February 1999, pp. 37–42.

31. T. Wilson, "E-Biz Bucks Lost Under the SSL Train," *Internet Week,* May 24, 1999, pp. 1, 3.

32. H. Gilbert, "Introduction to TCP/IP," February 2, 1995 <www.yale.edu/pclt/COMM/TCPIP.HTM>.

33. RSA Laboratories, "Security Protocols Overview," 1999 <www.rsasecurity.com/standards/protocols>.

34. Update M. Bull, "Ensuring End-to-End Security with SSL," *Network World,* May 15, 2000, p. 63.

35. <www.cisco.com/warp/public/44/solutions/network/vpn.shtml>.

36. S. Burnett and S. Paine, *RSA Security's Official Guide to Cryptography,* Berkeley: Osborne/McGraw-Hill, 2001, p. 210.

37. D. Naik, *Internet Standards and Protocols,* Microsoft Press 1998, pp. 79–80.

38. M. Grayson, "End the PDA Security Dilemma," *Communication News,* February 2001, pp. 38–40.

39. T. Wilson, "VPNs Don't Fly Outside Firewalls," *Internet Week,* May 28, 2001.

40. A. Eisenberg, "Viruses Could Have Your Numbers," *The New York Times,* June 8, 2000, p. 5.

41. D. Herbeck, Chair and Associate Professor of Communications, Boston College, February 29, 2000, lecture notes.

42. M.J. McCarthy, "Thinking Out Loud: You Assumed Erase Wiped Out That Rant Against the Boss.? Nope," *The Wall Street Journal,* March 7, 2000.

43. *Webster's New World College Dictionary,* New York: Mcmillan, 1999.

44. <www.abbottlaw.com>.

45. *Miller v. California* 413 U.S. 15 at 24–25 (1973).

46. *FCC v. Pacifica Foundation* 438 U.S. 726 (1978).

47. T. Reason, "Besieged by Spam," *CFO,* April 15, 2003, pp. 25–26.

48. S. Scalet, "The Pirates Among Us," *CIO,* April 15, 2003, pp. 87–92.

49. S. Scalet, "The Pirates Among Us," *CIO,* April 15, 2003, pp. 87–92.

50. L. Lessig, "Patent Problems," *The Industry Standard,* January 31, 2000, p. 47.

51. R. Libshon, "Madness In the Method: Will Method of Doing Business' Patents Undermine the Web? *Net Commerce Magazine,* March 2000, p. 8.

52. R. Kwon, "Delivering Medical Records, Securely," *Internet World,* August 10, 1998, p. 23.

53. S. A. Pignone, "When Cell Phones Save Lives," *NEAR* Vol. 1, No. 2, pp. 11–14.

54. "First-to-Wireless™," WindWire, Inc., December 27, 2000, p. 2.

55. E. Newborne, "Look Ma! No Ads!," *Inside,* February 6, 2001, p. 81.

56. T. Bair, "True Tales of Mobile Advertising: The Need for Standards," Wireless Advertising Conference Atlanta, Georgia, May, pp. 20–23.

57. K. Bayne, "Wireless Devices: The New Marketing Frontier," *e-Business Advisor,* December 2000, p. 12.

58. D. Callaghan, "Marketers Targeting Mobile Buyers," *eWeek,* February 26, 2001, p. 35.

59. D. Drucker, "The Web: Hardly Death Of A Salesman," *InternetWeek,* October 25, 1999, p. 73.

60. "MeT Threatened by Mobile SET Payments?" March 7, 2001 <www.epaynews.com/archives/index.cgi?keywords=MeT&optional=&subject=&location=&ref=keyword&f=view&id=983973203212120150 50&block=2>.

61. J. Blau "Carriers, Banks Partner for Payments," *m-business,* April 2001, p. 37.

62. "Say. Buy It!: Nuance and Qpass Team to Offer Voice-Driven Commerce Services to Wireless Carriers with the Qpass TalkWallet™," Qpass Press Release, March 20, 2001.

63. C. Nobel and D. Callaghan, "Wireless Services Hit Snags," *eWeek,* December 18, 2000, p. 15.

64. M. Hamblen, "Ensuring Portable Privacy," *Computerworld,* December 11, 2000, p. 50.