CHAPTER 7

THE ENVIRONMENT OF ELECTRONIC COMMERCE: LEGAL, ETHICAL, AND TAX ISSUES

LEARNING OBJECTIVES

In this chapter, you will learn about:

- Laws that govern electronic commerce activities
- Laws that govern the use of intellectual property by online businesses
- Online crime, terrorism, and warfare
- Ethics issues that arise for companies conducting electronic commerce
- Conflicts between companies' desire to collect and use data about their customers and the privacy rights of those customers
- Taxes that are levied on electronic commerce activities

INTRODUCTION

In 1999, **Dell Computer** and Micron Electronics (now doing business as **MPC Computers**), two companies that sell personal computers through their Web sites, agreed to settle U.S. Federal Trade Commission (FTC) charges that they had disseminated misleading advertising to their existing and potential customers. The advertising in question was for computer leasing plans that both companies had offered on their Web sites. The ads stated the price of the computer along with a monthly payment.

Unfortunately for Dell and Micron, stating the monthly payment without disclosing full details of the lease plan is a violation of the Consumer Leasing Act of 1976. This law is implemented through a federal regulation that was written and is updated periodically by the Federal Reserve Board. This regulation, called Regulation M, was designed to require banks and other lenders to fully disclose the terms of leases so that consumers would have enough information to make informed financing choices when leasing cars, boats, furniture, and other goods.

Both Dell and Micron had included the required information on their Web pages, but FTC investigators noted that important details of the leasing plans, such as the number of payments and the fees due at the signing of the lease, were placed in a small typeface at the bottom of a long Web page. A consumer who wanted to determine the full cost of leasing a computer would need to scroll through a number of densely filled screens to obtain enough information to make the necessary calculations.

In the settlement, both companies agreed to provide consumers with clear, readable, and understandable information in their lease advertising. The companies also agreed to record-keeping and federal monitoring activities designed to ensure their compliance with the terms of the settlement.

Dell and Micron are computer manufacturers. It apparently did not occur to them that they needed to become experts in Regulation M, generally considered to be a banking regulation. Companies that do business on the Web expose themselves, often unwittingly, to liabilities that arise from today's business environment. That environment includes laws and ethical considerations that may be different from those with which the business is familiar. In the case of Dell and Micron, they were unfamiliar with the laws and ethics of the banking industry. The banking industry has a different culture than that of the computer industry—it is unlikely that a bank advertising manager would have made such a mistake.

As you will learn in this chapter, Dell and Micron are by no means the only Web businesses that have run afoul of laws and regulations. As new and existing companies open online operations, they become subject to unfamiliar laws and different ethical frameworks much more rapidly than in the physical world.

THE LEGAL ENVIRONMENT OF ELECTRONIC COMMERCE

Businesses that operate on the Web must comply with the same laws and regulations that govern the operations of all businesses. If they do not, they face the same set of penalties—fines, reparation payments, court-imposed dissolution, and even jail time for officers and owners—that any business faces.

Businesses operating on the Web face two additional complicating factors as they try to comply with the law. First, the Web extends a company's reach beyond traditional boundaries. As you learned in Chapter 1, a business that uses the Web immediately becomes an international business. Thus, a company can become subject to many more laws more quickly than a traditional brick-and-mortar business based in one specific physical location. Second, the Web increases the speed and efficiency of business communications. As you learned in Chapters 3 and 4, customers often have much more interactive and complex relationships with online merchants than they do with traditional merchants. Further, the Web creates a network of customers who often have significant levels of interaction with each other. Web businesses that violate the law or breach ethical standards can face rapid and intense reactions from many customers and other stakeholders who become aware of the businesses' activities.

In this section, you will learn about the issues of borders, jurisdiction, and Web site content and how these factors affect a company's ability to conduct electronic commerce. You will also learn about legal issues that arise when the Web is used in the commission of crimes, terrorist acts, and even the conduct of war.

Borders and Jurisdiction

Territorial borders in the physical world serve a useful purpose in traditional commerce: They mark the range of culture and reach of applicable laws very clearly. When people travel across international borders, they are made aware of the transition in many ways. For example, exiting one country and entering another usually requires a formal examination of documents, such as passports and visas. In addition, both the language and the currency usually change upon entry into a new country. Each of these experiences, and countless others, are manifestations of the differences in legal rules and cultural customs in the two countries. In the physical world, geographic boundaries almost always coincide with legal and cultural boundaries. The limits of acceptable ethical behavior and the laws that are adopted in a geographic area are the result of the influences of the area's dominant culture. The relationships among a society's culture, laws, and ethical standards appear in Figure 7-1.

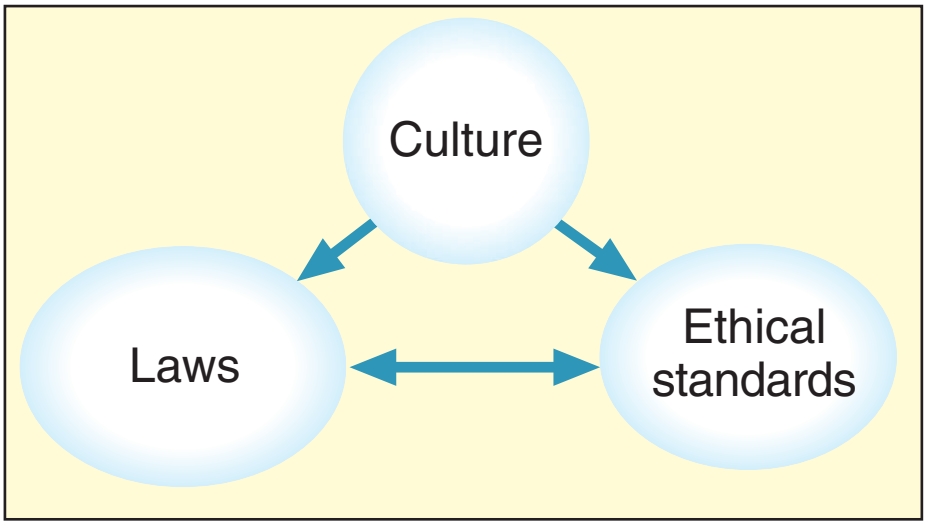

FIGURE 7-1 Culture helps determine laws and ethical standards

The geographic boundaries on culture are logical; for most of our history, humans have been unable to travel great distances to learn about other cultures. In recent years, however, some countries decided that times have indeed changed, and people can travel easily from one country to another within a geographic region. One example is the European Union (EU), which allows free movement within the EU for citizens of member countries. Most of the EU countries (Great Britain being a notable exception) have even formed the European Money Union and use a common currency (the euro) instead of their former individual currencies (for example, French francs, German marks, and Italian lire). Legal scholars define the relationship between geographic boundaries and legal boundaries in terms of four elements: power, effects, legitimacy, and notice.

Power

Power is a form of control over physical space and the people and objects that reside in that space, and is a defining characteristic of statehood. For laws to be effective, a government must be able to enforce them. Effective enforcement requires the power both to exercise physical control over residents, if necessary, and to impose sanctions on those who violate the law. The ability of a government to exert control over a person or corporation is called **jurisdiction**.

Laws in the physical world do not apply to people who are not located in or do not own assets in the geographic area that created those particular laws. For example, the United States cannot enforce its copyright laws on a citizen of Japan who is doing business in Japan and owns no assets in the United States. Any assertion of power by the United States over such a Japanese citizen would conflict with the Japanese government's recognized monopoly on using force with its citizens. Japanese citizens who bring goods into the United States to sell, however, are subject to applicable U.S. copyright laws. A Japanese Web site that offers delivery of goods into the United States is, similarly, subject to applicable U.S. laws.

The level of power asserted by a government is limited to that which is accepted by the culture that exists within its geographic boundaries. Ideally, geographic boundaries, cultural groupings, and legal structures all coincide. When they do not, internal strife and civil wars can erupt.

Effects

Laws in the physical world are grounded in the relationship between physical proximity and the **effects**, or impact, of a person's behavior. Personal or corporate actions have stronger effects on people and things that are nearby than on those that are far away. Government-provided trademark protection is a good example of this. For instance, the Italian government can provide and enforce trademark protection for a business named Casa di Baffi located in Rome. The effects of another restaurant using the same name are strongest in Rome, somewhat less in geographic areas close to Rome, and even less in other parts of Italy. That is, the effects diminish as geographic distance increases. If someone were to open a restaurant in Kansas City and call it Casa di Baffi, the restaurant in Rome would experience few, if any, negative effects from the use of its trademarked name in Kansas City because it would be so far away and because so few people would be potential customers of both restaurants. Thus, the effects of the trademark violation are controlled by Italian law because of the limited range within which such a violation has an effect.

The characteristics of laws are determined by the local culture's acceptance or rejection of various kinds of effects. For example, certain communities in the United States require that houses be built on lots that are at least 5 acres. Other communities prohibit outdoor advertising of various kinds. The local cultures in these communities make the effects of such restrictions acceptable.

When businesses begin operations online, the traditional measures of effects—and the laws that have been developed using those measures over many years—do not work very well. For example, France has a law that prohibits the sale of Nazi memorabilia. The people of France have considered this to be a reasonable law for many years. U.S. laws do not include a similar prohibition. When U.S.-based online auction sites began hosting auctions of Nazi memorabilia, those sites were in compliance with U.S. laws. However, because of the international nature of the Web, these auctions were available to people around the world, including residents of France. The French government ordered Yahoo! Auctions to stop these auctions. Yahoo! argued that it was in compliance with U.S. law, but the French government insisted that the effects of those Yahoo! auctions extended to France and thus violated French law. To avoid protracted legal actions over the jurisdiction issue, Yahoo! decided that it would no longer carry such auctions (*Note:* If you search in Yahoo! auctions using terms such as "Nazi," you might find some items available. These items, which include coins and stamps, are not considered Nazi memorabilia under French law.)

Legitimacy

Most people agree that the legitimate right to create and enforce laws derives from the mandate of those who are subject to those laws. In 1970, the **United Nations** passed a resolution that affirmed this idea of governmental legitimacy. The resolution made clear that the people residing within a set of recognized geographic boundaries are the ultimate source

of legitimate legal authority for people and actions within those boundaries. Thus, **legitimacy** is the idea that those subject to laws should have some role in formulating them.

Some cultures allow their governments to operate with a high degree of autonomy and unquestioned authority. China and Singapore are countries in which national culture permits the government to exert high levels of unchecked authority. Other cultures, such as those of the Scandinavian countries, place strict limits on governmental authority.

The levels of authority and autonomy with which governments of various countries operate varies significantly from one country to another. Online businesses must be ready to deal with a wide variety of regulations and levels of enforcement of those regulations as they expand their businesses to other countries. This can be difficult for smaller businesses that operate on the Web.

Notice

Physical boundaries are a convenient and effective way to announce the ending of one legal or cultural system and the beginning of another. The physical boundary, when crossed, provides **notice** that one set of rules has been replaced by a different set of rules. Notice is the expression of such a change in rules. People can obey and perceive a law or cultural norm as fair only if they are notified of its existence. Borders provide this notice in the physical world. The legal systems of most countries include a concept called constructive notice. People receive **constructive notice** that they have become subject to new laws and cultural norms when they cross an international border, even if they are not specifically warned of the changed laws and norms by a sign or a border guard's statement. Thus, ignorance of the law is not a sustainable defense, even in a new and unfamiliar jurisdiction.

This presents particular problems for online businesses, because they may not know that customers from another country are accessing their Web sites. Thus, the concept of notice—even constructive notice—does not translate very well to online business.

Jurisdiction on the Internet

Defining, establishing, and asserting jurisdiction are much more difficult on the Internet than they are in the physical world, mainly because traditional geographic boundaries do not exist. For example, a Swedish company that engages in electronic commerce may have a Web site that is entirely in English and a URL that ends in ".com," thus not indicating to customers that it is a Swedish firm. The server that hosts this company's Web page could be in Canada, and the people who maintain the Web site might work from their homes in Australia.

If a Mexican citizen buys a product from the Swedish firm and is unhappy with the goods received, that person might want to file a lawsuit against the seller firm. However, the world's physical border-based systems of law and jurisdiction do not help this Mexican citizen determine where to file the lawsuit. The Internet does not provide anything like the obvious international boundary lines in the physical world. Thus, the four considerations that work so well in the physical world—power, effects, legitimacy, and notice—do not translate very well to the virtual world of electronic commerce.

Governments that want to enforce laws regarding business conduct on the Internet must establish jurisdiction over that conduct. A **contract** is a promise or set of promises between two or more legal entities—people or corporations—that provides for an

exchange of value (goods, services, or money) between or among them. If either party to a contract does not comply with the terms of the contract, the other party can sue for failure to comply, which is called **breach of contract**. Persons and corporations that engage in business are also expected to excercise due care and not violate laws that prohibit specific actions (such as trespassing, libel, or professional malpractice). A **tort** is an intentional or negligent action (other than breach of contract) taken by a legal entity that causes harm to another legal entity. People or corporations that wish to enforce their rights based on either contract or tort law must file their claims in courts with jurisdiction to hear their cases. A court has sufficient jurisdiction in a matter if it has both subject-matter jurisdiction and personal jurisdiction.

Subject-Matter Jurisdiction

Subject-matter jurisdiction is a court's authority to decide a particular type of dispute. For example, in the United States, federal courts have subject-matter jurisdiction over issues governed by federal law (such as bankruptcy, copyright, patent, and federal tax matters), and state courts have subject-matter jurisdiction over issues governed by state laws (such as professional licensing and state tax matters). If the parties to a contract are both located in the same state, a state court has subject-matter jurisdiction over disputes that arise from the terms of that contract. The rules for determining whether a court has subject-matter jurisdiction are clear and easy to apply. Few disputes arise over subject-matter jurisdiction.

Personal Jurisdiction

Personal jurisdiction is, in general, determined by the residence of the parties. A court has personal jurisdiction over a case if the defendant is a resident of the state in which the court is located. In such cases, the determination of personal jurisdiction is straightforward. However, an out-of-state person or corporation can also voluntarily submit to the jurisdiction of a particular state court by agreeing to do so in writing or by taking certain actions in the state.

One of the most common ways that people voluntarily submit to a jurisdiction is by signing a contract that includes a statement, known as a **forum selection clause**, that the contract will be enforced according to the laws of a particular state. That state then has personal jurisdiction over the parties who signed the contract regarding any enforcement issue that arises from the terms of that contract. Figure 7-2 shows a portion of the contract that governs site visitors' activities on the **Qpass** site. Qpass sells software to wireless system and network operating companies. The first paragraph shown includes the site's forum selection clause. The second paragraph clarifies that site visitors are subject to their own jurisdictions' laws in addition to the jurisdiction specified in the forum selection clause.

> These terms of use shall be governed by and construed in accordance with the laws of the State of Washington, without regard to its conflict of laws rules. Any legal action arising out of this Agreement shall be litigated and enforced under the laws of the State of Washington. In addition, you agree to submit to the jurisdiction of the courts of the State of Washington, and that any legal action pursued by you shall be within the exclusive jurisdiction of the courts of King County in the State of Washington.

FIGURE 7-2 Forum selection clause on the Qpass Web site

In the United States, individual states have laws that can create personal jurisdiction for their courts. The details of these laws, called **long-arm statutes**, vary from state to state, but generally create personal jurisdiction over nonresidents who transact business or commit tortious acts in the state. For example, suppose that an Arizona resident drives recklessly while in California and, as a result, causes a collision with another vehicle that is driven by a California resident. Due to the driver's tortious behavior in the state of California, the Arizona resident can expect to be called into a California court. In other words, California's long-arm statute gives its courts personal jurisdiction over the matter.

Businesses should be aware of jurisdictional considerations when conducting electronic commerce over state and international lines. In most states, the extent to which these laws apply to companies doing business over the Internet is unclear. Because these procedural laws were written before electronic commerce existed, their application to Internet transactions continues to evolve as more and more disputes arise from online commercial transactions. The trend in this evolving law is that the more business activities a company conducts in a state, the more likely it is that a court will assert personal jurisdiction over that company through the application of a long-arm statute.

One exception to the general rule for determining personal jurisdiction occurs in the case of tortious acts. A business can commit a tortious act by selling a product that causes harm to a buyer. The tortious act can be negligent, in which the seller unintentionally provides a harmful product, or it can be an intentional tort, in which the seller knowingly or recklessly causes injury to the buyer. The most common business-related intentional torts involve defamation, misrepresentation, fraud, and theft of trade secrets. Although case law is rapidly developing in this area also, courts tend to invoke their respective states' long-arm statutes much more readily in the case of tortious acts than in breach of contract cases. If the matter involves an intentional tort or a criminal act, courts will assert jurisdiction more liberally.

Jurisdiction in International Commerce

Jurisdiction issues that arise in international business are even more complex than the rules governing personal jurisdiction across state lines within the United States. The exercise of jurisdiction across international borders is governed by treaties between the countries engaged in the dispute. In general, U.S. courts determine personal jurisdiction for foreign companies and people in much the same way that these courts interpret the long-arm statutes in domestic matters. Non-U.S. corporations and individuals can be sued in U.S. courts if they conduct business or commit tortious acts in the United States. Similarly, foreign

courts can enforce decisions against U.S. corporations or individuals through the U.S. court system if those courts can establish jurisdiction over the matter.

Courts asked to enforce the laws of other nations sometimes follow a principle called **judicial comity**, which means that they voluntarily enforce other countries' laws or judgments out of a sense of comity, or friendly civility. However, most courts are reluctant to serve as forums for international disputes. Also, courts are designed to deal with weighing evidence and making findings of right and wrong. International disputes often require diplomacy and the weighing of costs and benefits. Courts are not designed to do cost-benefit evaluations and cannot engage in negotiation and diplomacy. Thus, courts (especially U.S. courts) prefer to have the executive branch of the government (primarily the State Department) negotiate international agreements and resolve international disputes.

Jurisdictional issues are complex and change rapidly. Any business that intends to conduct electronic commerce should consult an attorney who is well versed in these procedural issues. However, there are a number of resources online that can be useful to non-lawyers who want to do preliminary investigation of a legal topic such as jurisdiction. The Harvard Law School's **Berkman Center for Internet & Society** Web site includes links to many current Internet-related legal issues. The **UCLA Online Institute for Cyberspace Law and Policy** contains an archive of legal reference materials published between 1995 and 2002.

Conflict of Laws

In the United States, business is governed by federal laws, state laws, and local laws. Sometimes, these laws address the same issues in different ways. Lawyers call this situation a **conflict of laws**. Since online businesses usually serve broad markets that span many localities and many states, they generally look to federal laws for guidance. On occasion, this can lead to problems with state and local laws.

One online business that faced a serious conflict of laws problem was the direct wine sales industry. Most U.S. states have heavily regulated all types of alcoholic beverage sales since the repeal of prohibition in 1933. The U.S. Constitution's Commerce Clause prohibits the states from passing laws that interfere with interstate commerce. However, the states do have the right to regulate matters pertaining to the health and welfare of their citizens. Under this right, most states have laws that require alcoholic beverages be sold through a regulated system of producers, wholesalers, and retailers. Some states allowed producers (such as wineries) to sell directly to the public, but only within that state. When online wine stores wanted to sell their products across state lines, they ran into these laws. Some states allowed the sales, others allowed the sales if the online store delivered to a licensed retailer in the destination state, and some states prohibited all direct sales. This resulted in a classic conflict of laws. State laws regulated the sale of alcoholic beverages in the interest of the health and welfare of the state's citizens, yet those same laws gave in-state producers an advantage over out-of-state producers (in some states, in-state producers could sell direct without adding the markup of a retailer; in other states, out-of-state producers could not compete at all). When a state law gives an in-state business an advantage over an out-of-state business, the free flow of interstate commerce is impeded and, in general, the U.S. Constitution's Commerce Clause is violated.

For years, the online wine industry worked to find a way to resolve these issues with the states, but did not have much success. Finally, wineries filed suit on the Commerce

Clause violation issue. In 2005, the U.S. Supreme Court voted 5-4 to strike down Michigan and New York laws that barred out-of-state wineries from selling directly to consumers. The online wine industry was happy with the outcome, as were wine lovers throughout the country who could now buy wine directly from the more than 3000 wineries and online wine shops.

Contracting and Contract Enforcement in Electronic Commerce

Any contract includes three essential elements: an offer, an acceptance, and consideration. The contract is formed when one party accepts the offer of another party. An **offer** is a commitment with certain terms made to another party, such as a declaration of willingness to buy or sell a product or service. An offer can be revoked as long as no payment, delivery of service, or other consideration has been accepted. An **acceptance** is the expression of willingness to take an offer, including all of its stated terms. **Consideration** is the agreed-upon exchange of something valuable, such as money, property, or future services. When a party accepts an offer based on the exchange of valuable goods or services, a contract has been created. An **implied contract** can also be formed by two or more parties that act as if a contract exists, even if no contract has been written and signed.

People enter into contracts on a daily, and often hourly, basis. Every kind of agreement or exchange between parties, no matter how simple, is a type of contract. For example, every time a consumer buys an item at the supermarket, the elements of a valid contract are met:

- The store offers an item at a stated price.
- The consumer accepts this offer by indicating a willingness to buy the product for the stated price.
- The store exchanges its product for another valuable item: the consumer's payment.

Contracts are a key element of traditional business practice, and they are equally important on the Internet. Offers and acceptances can occur when parties exchange e-mail messages, engage in electronic data interchange (EDI), or fill out forms on Web pages. These Internet communications can be combined with traditional methods of forming contracts, such as the exchange of paper documents, faxes, and verbal agreements made over the telephone or in person. An excellent resource for many of the laws concerning contracts, especially as they pertain to U.S. businesses, is the Cornell Law School Web site, which includes the full text of the **Uniform Commercial Code (UCC)**.

When a seller advertises goods for sale on a Web site, that seller is not making an offer, but is inviting offers from potential buyers. If a Web ad were a legal offer to form a contract, the seller could easily become liable for the delivery of more goods than it has available to ship. When a buyer submits an order, which is an offer, the seller can accept that offer and create a contract. If the seller does not have the ordered items in stock, the seller has the option of refusing the buyer's order outright or counteroffering with a decreased amount. The buyer then has the option to accept the seller's counteroffer.

Making a legal acceptance of an offer is quite easy to do in most cases. When enforcing contracts, courts tend to view offers and acceptances as actions that occur within a particular context. If the actions are reasonable under the circumstances, courts tend to

interpret those actions as offers and acceptances. For example, courts have held that various actions—including mailing a check, shipping goods, shaking hands, nodding one's head, taking an item off a shelf, or opening a wrapped package—are all, in some circumstances, legally binding acceptances of offers. Although the case law is limited regarding acceptances made over the Internet, it is reasonable to assume that courts would view clicking a button on a Web page, entering information in a Web form, or downloading a file to be legally binding acceptances.

Written Contracts on the Web

In general, contracts are valid even if they are not in writing or signed. However, certain categories of contracts are not enforceable unless the terms are put into writing and signed by both parties. In 1677, the British Parliament enacted a law that specified the types of contracts that had to be in writing and signed. Following this British precedent, every state in the United States today has a similar law, called a **Statute of Frauds**. Although these state laws vary slightly, each Statute of Frauds specifies that contracts for the sale of goods worth more than $500 and contracts that require actions that cannot be completed within one year must be created by a signed writing. Fortunately for businesses and people who want to form contracts using electronic commerce, a writing does not require either pen or paper.

Most courts will hold that a **writing** exists when the terms of a contract have been reduced to some tangible form. An early court decision in the 1800s held that a telegraph transmission was a writing. Later courts have held that tape recordings of spoken words, computer files on disks, and faxes are writings. Thus, the parties to an electronic commerce contract should find it relatively easy to satisfy the writing requirement. Courts have been similarly generous in determining what constitutes a signature. A **signature** is any symbol executed or adopted for the purpose of authenticating a writing. Courts have held names on telegrams, telexes, faxes, and Western Union Mailgrams to be signatures. Even typed names or names printed as part of a letterhead have served as signatures. It is reasonable to assume that a symbol or code included in an electronic file would constitute a signature. As you will learn in Chapter 10, the United States now has a law that explicitly makes digital signatures legally valid for contract purposes.

Firms conducting international electronic commerce do not need to worry about the signed writing requirement in most cases. The main treaty that governs international sales of goods, Article 11 of the United Nations Convention on Contracts for the International Sale of Goods (CISG), requires neither a writing nor a signature to create a legally binding acceptance. You can learn more about the CISG and related topics in international commercial law at the **Pace University School of Law CISG Information** Web site.

Warranties on the Web

Most firms conducting electronic commerce have little trouble fulfilling the requirements needed to create enforceable, legally binding contracts on the Web. One area that deserves attention, however, is the issue of warranties. Any contract for the sale of goods includes implied warranties. A seller implicitly warrants that the goods it offers for sale are fit for the purposes for which they are normally used. If the seller knows specific information about the buyer's requirements, acceptance of an offer from that buyer may result in an additional implied warranty of fitness, which suggests that the goods are suitable for the specific uses of that buyer. Sellers can also create explicit warranties by providing a specific description of the additional warranty terms. It is also possible for a seller to create explicit warranties, often unintentionally, by making general statements in brochures or other advertising materials about product performance or suitability for particular tasks.

Sellers can avoid some implied warranty liability by making a warranty disclaimer. A **warranty disclaimer** is a statement declaring that the seller will not honor some or all implied warranties. Any warranty disclaimer must be conspicuously made in writing, which means it must be easily noticed in the body of the written agreement. On a Web page, sellers can meet this requirement by putting the warranty disclaimer in larger type, a bold font, or a contrasting color. To be legally effective, the warranty disclaimer must be stated obviously and must be easy for a buyer to find on the Web site. Figure 7-3 shows a portion of an **Apple Computer** Web page that includes the warranty disclaimer for its Web site. The warranty disclaimer is printed in uppercase letters to distinguish it from other text on the page.

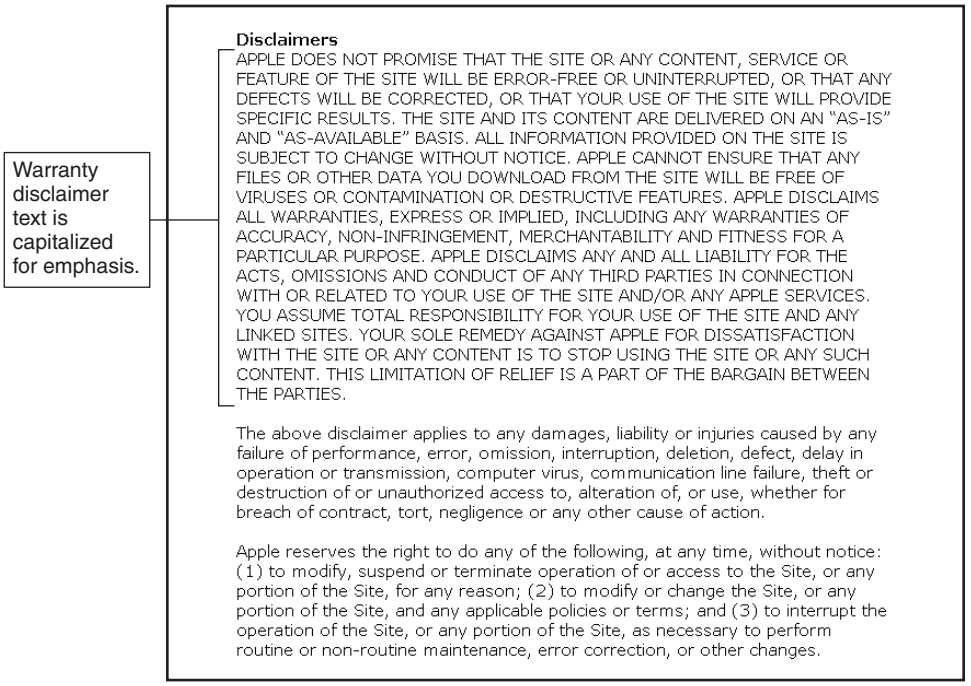

FIGURE 7-3 Apple Computer Web site warranty disclaimer

Authority to Form Contracts

As explained previously in this section, a contract is formed when an offer is accepted for consideration. Problems can arise when the acceptance is issued by an imposter or someone who does not have the authority to bind the company to a contract. In electronic commerce, the online nature of acceptances can make it relatively easy for identity forgers to pose as others.

Fortunately, the Internet technology that makes forged identities so easy to create also provides the means to avoid being deceived by a forged identity. In Chapter 10, you will learn how companies and individuals can use digital signatures to establish identity in online transactions. If the contract is for any significant amount, the parties should require each other to use digital signatures to avoid identity problems. In general, courts will not hold a person or corporation whose identity has been forged to the terms of the contract; however, if negligence on the part of the person or corporation contributed to the forgery, a court may hold the negligent party to the terms of the contract. For example, if a company was careless about protecting passwords and allowed an imposter to enter the company's system and accept an offer, a court might hold that company responsible for fulfilling the terms of that contract.

Determining whether an individual has the authority to commit a company to an online contract is a greater problem than forged identities in electronic commerce. This issue, called **authority to bind**, can arise when an employee of a company accepts a contract and the company later asserts that the employee did not have such authority. For large transactions in the physical world, businesses check public information on file with the state of incorporation, or ask for copies of corporate certificates or resolutions, to establish the authority of persons to make contracts for their employers. These methods are available to parties engaged in online transactions; however, they can be time consuming and awkward. You will learn about some good electronic solutions, such as digital signatures and certificates from a certification authority, in Chapter 10.

Terms of Service Agreements

Many Web sites have stated rules that site visitors must follow, although most visitors are not aware of these rules. If you examine the home page of a Web site, you will often find a link to a page titled "Terms of Service," "Conditions of Use," "User Agreement," or something similar. If you follow that link, you find a page full of detailed rules and regulations, most of which are intended to limit the Web site owner's liability for what you might do with information you obtain from the site. These contracts are often called **terms of service (ToS)** agreements even when they appear under a different title. In most cases, a site visitor is held to the terms of service even if that visitor has not read the text or clicked a button to indicate agreement with the terms. The visitor is bound to the agreement by simply using the site. The first few sections of the Amazon.com terms of service agreement appear in Figure 7-4, which shows the top of Amazon's Conditions of Use page.

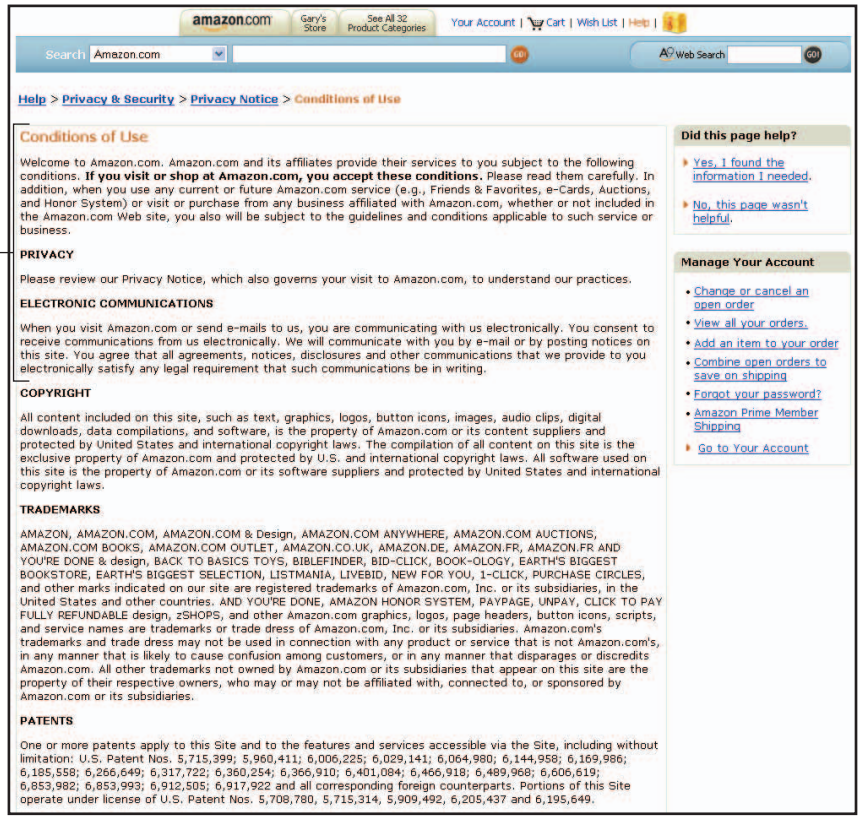

FIGURE 7-4 Amazon.com conditions of use page

USE AND PROTECTION OF INTELLECTUAL PROPERTY IN ONLINE BUSINESS

Online businesses must be careful in their use of intellectual property. **Intellectual property** is a general term that includes all products of the human mind. These products can be tangible or intangible. Intellectual property rights include the protections afforded to individuals and companies by governments through governments' granting of copyrights and patents, and through registration of trademarks and service marks. Online businesses must take care to avoid deceptive trade practices, false advertising claims, defamation or product disparagement, and violations of intellectual property rights by using unauthorized content on their Web sites or in their domain names.

Web Site Content Issues

A number of legal issues can arise regarding the Web page content of electronic commerce sites. The most common concerns involve the use of intellectual property that is protected by other parties' copyrights, patents, trademarks, and service marks.

Copyright Infringement

A **copyright** is a right granted by a government to the author or creator of a literary or artistic work. The right is for the specific length of time provided in the copyright law and gives the author or creator the sole and exclusive right to print, publish, or sell the work. Creations that can be copyrighted include virtually all forms of artistic or intellectual expression—books, music, artworks, recordings (audio and video), architectural drawings, choreographic works, product packaging, and computer software. In the United States, works created after 1977 are protected for the life of the author plus 70 years. Works copyrighted by corporations or not-for-profit organizations are protected for 95 years from the date of publication or 120 years from the date of creation, whichever is earlier.

The idea contained in an expression cannot be copyrighted. It is the particular form in which an idea is expressed that creates a work that can be copyrighted. If an idea cannot be separated from its expression in a work, that work cannot be copyrighted. For example, mathematical calculations cannot be copyrighted. A collection of facts can be copyrighted, but only if the collection is arranged, coordinated, or selected in a way that causes the resulting work to rise to the level of an original work. For example, the Yahoo! Web Directory is a collection of links to URLs. These facts existed before Yahoo! selected and arranged them into the form of its directory. However, most copyright lawyers would argue that the selection and arrangement of the links into categories probably makes the directory copyrightable.

In the past, many countries (including the United States) required the creator of a work to register that work to obtain copyright protection. U.S. law still allows registration, but registration is no longer required. A work that does not include the words "copyright" or "copyrighted," or the copyright symbol ©, but was created after 1977, is copyrighted automatically by virtue of the copyright law unless the creator specifically released the work into the public domain.

Most U.S. Web pages are protected by the automatic copyright provision of the law because they arrange the elements of words, graphics, and HTML tags in a way that creates an original work (in addition, many Web pages have been registered with the U.S. Copyright Office). This creates a potential problem because of the way the Web works. As you learned in Chapter 2, when a Web client requests a page, the Web server sends an HTML file to the client. Thus, a copy of the HTML file (along with any graphics or other files needed to render the page) resides on the Web client computer. Most legal experts agree that this copying is a fair use of the copyrighted Web page. The U.S. copyright law includes an exemption from infringement actions for fair use of copyrighted works. The **fair use** of a copyrighted work includes copying it for use in criticism, comment, news reporting, teaching, scholarship, or research. The law's definition of fair use is intentionally broad and can be difficult to interpret. When you make fair use of a copyrighted work, you must be careful to provide a citation to the original work to avoid charges of plagiarism. The **University of Texas Crash Course in Copyright** is a particularly helpful source of information on making fair use determinations.

Copyright law has always included elements, such as the fair use exemption, that make it difficult to apply. The Internet has made this situation worse because it allows the immediate transmission of exact digital copies of many materials. In the case of digital music, the Napster site provided a network that millions of people used to trade music files that

they had copied from their CDs and compressed into MPEG version 3 format, commonly referred to as MP3. This constituted copyright violation on a grand scale, and a group of music recording companies sued Napster for facilitating the violations.

Napster argued that it had only provided the "machinery" used in the copyright violations—much as electronics companies manufacture and sell VCRs that might be used to make illegal copies of videotapes—and had not itself infringed on any copyrights. Both the U.S. District Court and the Federal Appellate Court held that Napster was guilty of vicarious copyright infringement, even though it did not directly violate any music recording companies' copyrights. An entity becomes liable for **vicarious copyright infringement** if it is capable of supervising the infringing activity and obtains a financial benefit from the infringing activity. Napster failed to monitor its network even though it could have done so. It also profited (by selling advertising on its Web site) indirectly from the infringement. Thus Napster was held liable even though Napster itself did not transfer any copies. The courts ordered that Napster be shut down. In late 2001, Napster agreed to pay $26 million in damages for copyright infringement to a group of music publishing associations and began working on relaunching the site with agreements in place to pay copyright holders for the music that would be downloaded in the future. After Napster filed for bankruptcy in 2002, software company **Roxio** bought all of Napster's intellectual property, including its name and Web site, for about $5 million. Roxio launched a new **Napster** site in October 2003. The site now offers legal music downloads to subscribers.

With the growth in popularity of portable music devices such as Apple's iPod, the demand for music in the MP3 (and similar) formats has continued to increase. The companies that sell music downloads, such as the new Napster site, Apple's **iTunes** site, and the **Yahoo! Music** site, each have different rules and restrictions that come with the downloaded files. Some sites allow one copy to be installed on a portable music device. Others allow a limited number of copies to be installed. Still others allow unlimited copies, but only if the devices on which the copies are installed are owned by the person who downloaded the file.

The legality of the common practice of copying files from music CDs and placing those files on a portable music device (or onto another CD) is unclear in many cases. This type of copying is governed in the United States by the fair use provisions of the copyright laws, which you learned about earlier in this chapter. The fair use provisions as they relate to copying music tracks are, at best, unclear and difficult to interpret. Some lawyers would argue that a person has the right under the fair use provisions to make a backup copy of a music CD track, but other lawyers would disagree. A person who makes one copy for a portable music device, a second copy for a computer, and a third copy on a CD for backup purposes would be less likely to be protected under the fair use provisions, but some lawyers would argue that all three are protected uses.

Patent Infringement

A **patent** is an exclusive right granted by the government to an individual to make, use, and sell an invention. In the United States, patents on inventions protect the inventor's rights for 20 years. A patent on the design for an invention provides protection for 14 years. To be patentable, an invention must be genuine, novel, useful, and not obvious given the current state of technology. In the early 1980s, companies began obtaining patents on software programs that met the terms of the U.S. patent law. However, most firms that develop

software to use in Web sites and for related transaction processing have not found the patent law to be very useful. The process of obtaining a patent is expensive and can take several years. Most developers of Web-related software believe that the technology in the software could become obsolete before the patent protection is secured.

One type of patent has been of interest to companies engaging in electronic commerce. A U.S. Court of Appeals ruled in 1998 that patents could be granted on "methods of doing business." The **business process patent**, which protects a specific set of procedures for conducting a particular business activity, is quite controversial. In addition to the Amazon.com patent on its 1-Click purchasing method (which you read about in Chapter 4), other Web businesses have obtained business process patents. The Priceline.com "name your own price" price-tendering system, About.com's approach to aggregating information from many different Web sites, and Cybergold's method of paying people to view its Web site have each received business process patents.

The ability of companies to enforce their rights under these patents is not yet clear. Many legal experts and business researchers believe that the issuance of business process patents grants the recipients unfair monopoly power and is an inappropriate extension of patent law. In 1999, Amazon.com sued Barnes & Noble for using a process on its Web site that was similar to the 1-Click method. The case was settled out of court in 2002, but the terms of the settlement were not disclosed. The U.S. Supreme Court has not yet ruled on any cases involving business process patents. To read an interesting discussion of both sides of the business process patent issue that includes exchanges between Jeff Bezos, founder of Amazon.com, and book publisher Tim O'Reilly, see the article posted at **My Conversation with Jeff Bezos**.

Trademark Infringement

A **trademark** is a distinctive mark, device, motto, or implement that a company affixes to the goods it produces for identification purposes. A **service mark** is similar to a trademark, but it is used to identify services provided. In the United States, trademarks and service marks can be registered with state governments, the federal government, or both. The name (or a part of that name) that a business uses to identify itself is called a **trade name**. Trade names are not protected by trademark laws unless the business name is the same as the product (or service) name. They are protected, however, under common law. **Common law** is the part of British and U.S. law established by the history of court decisions that has accumulated over many years. The other main part of British and U.S. law, called **statutory law**, arises when elected legislative bodies pass laws, which are also statutes.

The owners of registered trademarks have often invested a considerable amount of money in the development and promotion of their trademarks. Web site designers must be very careful not to use any trademarked name, logo, or other identifying mark without the express permission of the trademark owner. For example, a company Web site that includes a photograph of its president who happens to be holding a can of Pepsi could violate Pepsi's trademark rights. Pepsi can argue that the appearance of its trademarked product on the Web site implies an endorsement of the president or the company by Pepsi.

Domain Names, Cybersquatting, and Name Stealing

Considerable controversy has arisen recently about intellectual property rights and Internet domain names. **Cybersquatting** is the practice of registering a domain name that is the trademark of another person or company in the hopes that the owner will pay huge amounts of money to acquire the URL. In addition, successful cybersquatters can attract many site visitors and, consequently, charge high advertising rates. A related problem, called **name changing**, occurs when someone registers purposely misspelled variations of well-known domain names. These variants sometimes lure consumers who make typographical errors when entering a URL. **Name stealing** occurs when someone posing as a site's administrator changes the ownership of the site's assigned domain name to another site and owner. Name stealing is more of a nuisance than a serious problem because the act can be quickly identified and the ownership of the domain name switched back to the rightful owner before significant damage occurs.

Since 1999, the U.S. Anticybersquatting Consumer Protection Act has prevented businesses' trademarked names from being registered as domain names by other parties. The law provides for damages of up to $100,000 per trademark. If the registration of the domain name is found to be "willful," damages can be as much as $300,000. Recent U.S. cases that were settled out of court illustrate the problem. For example, three cybersquatters made headlines when they tried to sell the URL barrydiller.com for $10 million. Barry Diller, the CEO of USA Networks, sued the trio and won.

Registering a generic name such as Wine.com is very different from registering a trademarked name in bad faith—cybersquatting. Registering a generic name is legal speculation that the name might one day become valuable. Disputes that arise when one person has registered a domain name that is an existing trademark or company name are settled by the **World Intellectual Property Association (WIPO)**. The WIPO began settling domain name disputes in 1999 under its Uniform Domain Name Dispute Resolution Policy (UDRP).

One common type of dispute arises when a business has a trademark that is a common term. If a person obtains the domain name containing that common term, the owner of the trademark must seek resolution at the WIPO. In 2000, Gordon Sumner, who had then been performing music for more than 20 years as Sting, filed a complaint with the WIPO because a Georgia man obtained the domain name www.sting.com and had reportedly offered to sell it to Sting for $25,000. In more than 80 percent of its cases, the WIPO has held for the trademark name owner; however, in this case, the WIPO noted that the word "sting" was in common and general use and had multiple meanings other than as an identifier for the musician. The WIPO refused to award the domain to Sumner. After the WIPO decision, the two parties came to undisclosed terms and the musician's official Web site is now at www.sting.com.

Many critics have argued that the WIPO UDRP has been enforced unevenly and that many of the decisions under the policy have been inconsistent. One problem faced by those who have used the WIPO resolution service is that the WIPO decisions are not appealed to one authority. Instead, the party seeking redress must file suit in a court with the appropriate jurisdiction. No central authority maintains records of all WIPO decisions and appeals. You can learn more about WIPO UDRP decisions by reading the Harvard Law School's **Berkman Center UDRP Opinion Guide**. A complete list of all UDRP decisions with links to the text of each decision appears on the **ICANN UDRP Proceedings** Web pages.

After obtaining a domain name, companies still face the possibility that someone will steal unsuspecting customers by registering a domain name that is a slight variation, or even a misspelling, of a company's well-known domain name. A simple typo in a Web address could lead a Web surfer to LLBaen.com instead of LLBean.com. The Anticybersquatting Consumer Protection Act now helps distinguish between cases that are true cybersquatting and those that are permissible competition. Most businesses agree that the practice of name changing is annoying to affected online businesses and confusing to customers. A company's best defense is to register as many variations in product and company spellings as possible. Unfortunately, there is no complete solution to this problem; as new high-level domains such as .biz become available, the name-changing problem recurs.

Perhaps the most flagrant example of domain name abuse is name stealing. Name stealing occurs when someone other than a domain name's owner changes the ownership of the domain name. A **domain name ownership change** occurs when owner information maintained by a public domain registrar is changed in the registrar's database to reflect a new owner's name and business address. This usually happens only when safeguards are not in place. Once domain name ownership is changed, the name stealer can manipulate the site, post graffiti on it, or redirect online customers to other sites selling substandard goods. The main purpose of name stealing is to harass the site owner. The temporary loss of its domain name can cut off a business from its Web site for several days.

Protecting Intellectual Property Online

Several industry trade groups have proposed solutions to the current problems in digital copyright protection, including host name blocking, packet filtering, and proxy servers. All three approaches illustrate how an Internet service provider might try to block access to an entire offending site. However, none of these approaches are really effective in preventing theft or providing identification of property obtained without the copyright holder's permission.

Several methods show promise in the battle to protect digital works, but they only provide partial protection. New and improved methods are continually being developed. One promising technique employs steganography to create a **digital watermark**. The watermark is a digital code or stream embedded undetectably in a digital image or audio file. It can be encrypted to protect its contents, or simply hidden among the bits—digital information—comprising the image or recording. **Verance** is a company that provides, among other products, digital audio watermarking systems to protect audio files on the Internet. Its systems identify, authenticate, and protect intellectual property. Verance's ARIS MusiCode system enables recording artists to monitor, identify, and control the use of their digital recordings.

The audio watermarks do not alter the audio fidelity of the recordings in which they are embedded. The Verance SoniCode product provides verification and authentication tools. SoniCode was originally developed by ARIS Technologies, which is now owned by Verance Corporation. SoniCode can ensure that telephonic conversations have not been altered. The same is true for audiovisual transcripts and depositions. **Blue Spike** produces a watermarking system called Giovanni. Like the SoniCode system, the Giovanni watermark authenticates the copyright and provides copy control. **Copy control** is an electronic mechanism for limiting the number of copies that one can make of a digital work.

A group of more than 180 companies and organizations devoted to providing protection for intellectual property—digital music in this case—is the **Secure Digital Music Initiative (SDMI)** organization. Its members include information technology and consumer electronics companies, security technology firms, Internet service providers, and the music recording industry. SDMI's charter is to develop open, public technology specifications that protect the playing, storing, and distribution of digital music.

Digimarc is another company providing watermark protection systems and software. Its products embed a watermark that allows any works protected by its Digimarc system to be tracked across the Web. In addition, the watermark can link viewers to commerce sites and databases. It can also control software and playback devices. Finally, the imperceptible watermark contains copyright information and links to the image's creator, which enables nonrepudiation of a work's authorship and facilitates electronic purchase and licensing of the work.

Defamation

A **defamatory** statement is a statement that is false and that injures the reputation of another person or company. If the statement injures the reputation of a product or service instead of a person, it is called **product disparagement**. In some countries, even a true and honest comparison of products may give rise to product disparagement. Because the difference between justifiable criticism and defamation can be hard to determine, commercial Web sites should avoid making negative, evaluative statements about other persons or products.

Web site designers should be especially careful to avoid potential defamation liability by altering a photo or image of a person in a way that depicts the person unfavorably. In most cases, a person must establish that the defamatory statement caused injury. However, most states recognize a legal cause of action, called **per se defamation**, in which a court deems some types of statements to be so negative that injury is assumed. For example, the court will hold inaccurate statements alleging conduct potentially injurious to a person's business, trade, profession, or office as defamatory per se—the complaining party need not prove injury to recover damages. Thus, online statements about competitors should always be carefully reviewed before posting to determine whether they contain any elements of defamation.

An important exception in U.S. law exists for statements that are defamatory but that are about a public figure (such as a politician or a famous actor). The law allows considerable leeway for statements that are satirical or that are valid expressions of personal opinion. Other countries do not offer the same protections, so operators of Web sites with international audiences do need to be careful.

Also, recall that defaming or disparaging statements must be false. This protects Web sites that include unfavorable reviews of products or services if the statements made are not false. For example, if a person reads a book and believes it to be terrible, that person can safely post a review on Amazon.com that includes assessments of the book's lack of literary value. Such statements of personal opinion are true statements and thus neither defamatory nor disparaging.

Deceptive Trade Practices

The ease with which Web site designers can edit graphics, audio, and video files allows them to do many creative and interesting things. Manipulations of existing pictures, sounds, and video clips can be very entertaining. If the objects being manipulated are trademarked, however, these manipulations can violate the trademark holder's rights. Fictional characters can be trademarked or otherwise protected. Many personal Web pages include unauthorized use of cartoon characters and scanned photographs of celebrities; often, these images are altered in some way. A Web site that uses an altered image of Mickey Mouse speaking in a modified voice is likely to hear from the Disney legal team.

Web sites that include links to other sites must be careful not to imply a relationship with the companies sponsoring the other sites unless such a relationship actually exists. For example, a Web design studio's Web page may include links to company Web sites that show good design principles. If those company Web sites were not created by the design studio, the studio must be very careful to state that fact. Otherwise, it would be easy for a visitor to assume that the linked sites were the work of the design studio.

In general, trademark protection prevents another firm from using the same or a similar name, logo, or other identifying characteristic in a way that would cause confusion in the minds of potential buyers of the trademark holder's products or services. For example, the trademarked name "Visa" is used by one company for its credit card services and another company for its type of synthetic fiber. This use is acceptable because the two products are significantly different. However, the use of very well-known trademarks can be protected for all products if there is a danger that the trademark might be diluted. Various state laws define **trademark dilution** as the reduction of the distinctive quality of a trademark by alternative uses. Trademarked names such as "Hyatt," "Trivial Pursuit," and "Tiffany," and the shape of the Coca-Cola bottle have all been protected from dilution by court rulings. A Web site that sells gift-packaged seafood and claims to be the "Tiffany of the Sea" risks a lawsuit from the famous jeweler claiming trademark dilution.

Advertising Regulation

In the United States, advertising is regulated primarily by the **Federal Trade Commission**. The FTC publishes regulations and investigates claims of false advertising. Its Web site includes a number of information releases that are useful to businesses and consumers. The FTC business education campaign publications are available on its Advertising Guidance page, shown in Figure 7-5. These publications include information to help businesses comply with the law.

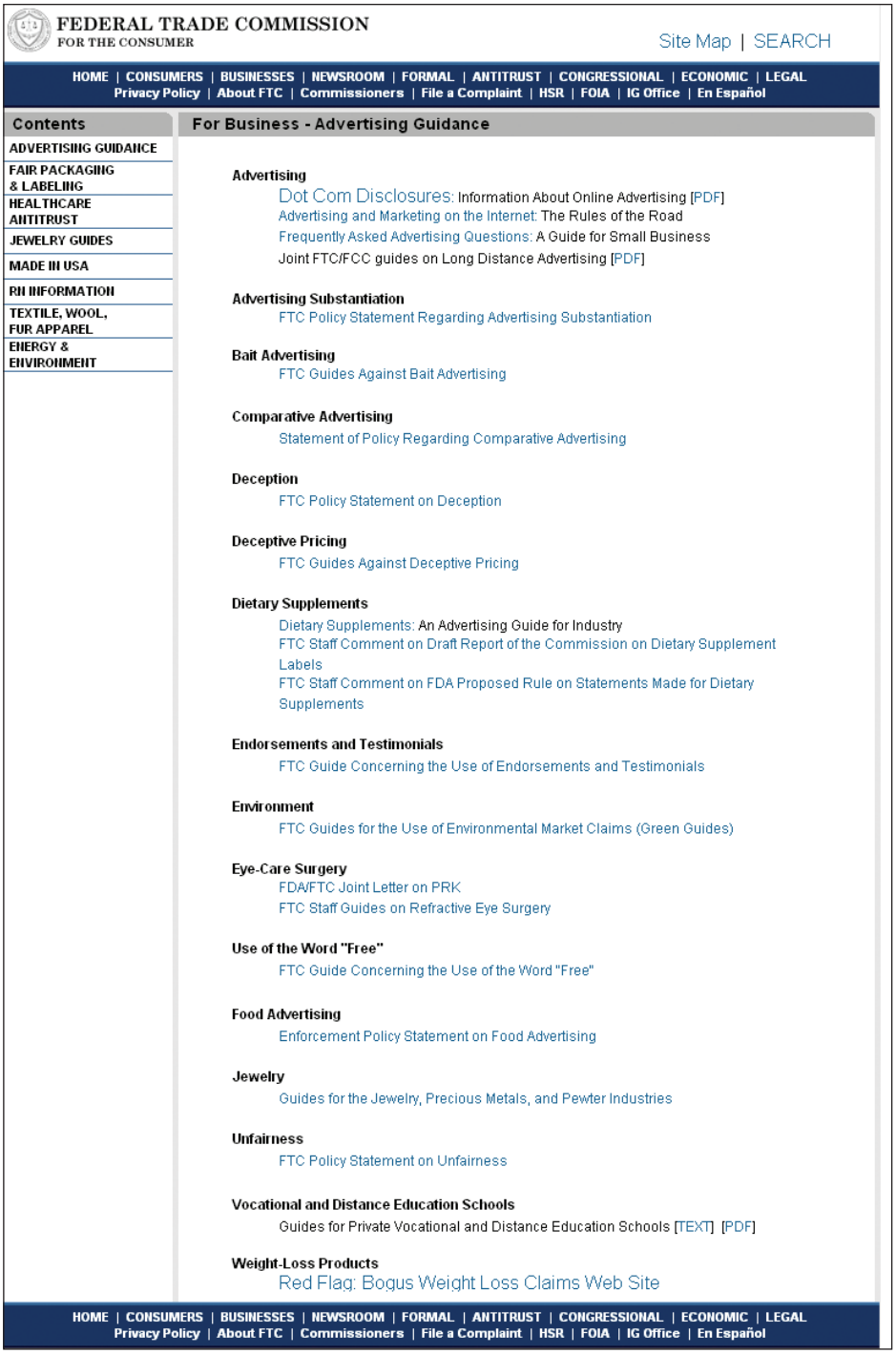

FIGURE 7-5 U.S. Federal Trade Commission Advertising Guidance page

Any advertising claim that can mislead a substantial number of consumers in a material way is illegal under U.S. law. In addition to conducting its own investigations, the FTC accepts referred investigations from organizations such as the Better Business Bureau. The FTC provides policy statements that can be helpful guides for designers creating electronic commerce Web sites. These policies include information on what is permitted in advertisements and cover specific areas such as these:

- Bait advertising
- Consumer lending and leasing
- Endorsements and testimonials
- Energy consumption statements for home appliances
- Guarantees and warranties
- Prices

Other federal agencies have the power to regulate online advertising in the United States. These agencies include the Food and Drug Administration (FDA), the Bureau of Alcohol, Tobacco, and Firearms (BATF), and the Department of Transportation (DOT). The FDA regulates information disclosures for food and drug products. In particular, any Web site that is planning to advertise pharmaceutical products will be subject to the FDA's drug labeling and advertising regulations. The BATF works with the FDA to monitor and enforce federal laws regarding advertising for alcoholic beverages and tobacco products. These laws require that every ad for such products includes statements that use very specific language. Many states also have laws that regulate advertising for alcoholic beverages and tobacco products. The state and federal laws governing advertising and the sale of firearms are even more restrictive. Any Web site that plans to deal in these products should consult with an attorney who is familiar with the relevant laws before posting any online advertising for such products. The DOT works with the FTC to monitor the advertising of companies over which it has jurisdiction, such as bus lines, freight companies, and airlines.

ONLINE CRIME, TERRORISM, AND WARFARE

The Internet has opened up many possibilities for people to communicate and get to know each other better—no matter where in the world they live. The Internet has also opened doors for businesses to reach new markets and create opportunities for economic growth. It is sad that some people in our world have found the Internet to be a useful tool for perpetrating crimes, conducting terrorism, and even waging war.

Online Crime

Crime on the Web includes online versions of crimes that have been undertaken for years in the physical world, including theft, stalking, distribution of pornography, and gambling. Other crimes, such as commandeering one computer to launch attacks on other computers, are new.

Law enforcement agencies have difficulty combating many types of online crime. The first obstacle they face is the issue of jurisdiction. As you learned earlier in this chapter, determining jurisdiction can be tricky on the Internet. Consider the case of a person living in Canada who uses the Internet to commit a crime against a person in Texas. It is unclear which elements of the crime could establish sufficient contact with Texas to allow police there to proceed against a citizen of a foreign country. It is possible that the actions that are considered criminal under Texas and U.S. law might not be considered so in Canada. If the crime is theft of intellectual property (such as computer software or computer files), the questions of jurisdiction become even more complex. You can learn more about online crime issues at the **U.S. Department of Justice Cybercrime** Web site.

Enforcing laws against distribution of pornographic material has also been difficult because of jurisdiction issues. The distinction between legal adult material and illegal pornographic material is, in many cases, subjective and often difficult to make. The U.S. Supreme Court has ruled that state and local courts can draw the line based on local community standards. This creates problems for Internet sales. For example, consider a case in which questionable adult content is sold on a Web site located in Oregon to a customer who downloads the material in Georgia. A difficult question arises regarding which community standards might apply to the sale.

A similar jurisdiction issue arises in the case of online gambling. Many gambling sites are located outside the United States. If people in California use their computers to connect to an offshore gambling site, it is unclear where the gambling activity occurs. Several states have passed laws that specifically outlaw Internet gambling, but the jurisdiction of those states to enforce laws that limit Internet activities is not yet clear.

Another problem facing law enforcement officers is the difficulty of applying laws that were written before the Internet became prevalent to criminal actions carried out on the Internet. For example, most states have stalking laws that provide criminal penalties to people who harass, annoy, or alarm another person in a way that presents a credible threat. Many of these laws are triggered by physical actions, such as physically following the person targeted. The Internet gives a stalker the opportunity to use e-mail or chat room discussions to create the threatening situation. Laws that require physical action on the part of the stalker are not effective against online stalkers. Only a few states have passed laws that specifically address the problem of online stalking.

An increasing number of companies have reported attempts by competitors and others to infiltrate their computer systems with the intent of stealing data or creating disruptions in their operations. Smaller companies are easier targets because they generally do not have strong security in place (you will learn more about security in electronic commerce in Chapter 10), but larger organizations are not immune to these attacks. In 2004, lawyer and computer expert Myron Tereshchuk was sentenced to five years in federal prison after pleading guilty to a charge of criminal extortion. Over a period of two years, he had been threatening a patent and trademark services company, MicroPatent, with disclosure of confidential client information and had demanded a payment of $17 million to "go away." He used a variety of means to hide his identity, but after more than a year of investigation by MicroPatent personnel and federal agents, he was identified and caught. When federal agents searched his home, they found firearms, hand grenades, and the ingredients needed to make ricin, a toxic gas used by terrorists. (In 2005, Tereshchuk pleaded guilty to

federal weapons charges that could add an additional 15 years to his sentence.) MicroPatent spent more than $500,000 on outside legal and technical consultants during the investigation and devoted significant internal resources to the effort. MicroPatent's sales managers also had to spend a tremendous amount of time with clients, reassuring them that their confidential information (details of their pending patent and trademark applications, for example) had not been compromised. MicroPatent's experience was not unusual. According to a 2004 Computer Security Institute survey of 634 companies, the average loss due to unauthorized data access was more than $300,000 and the average loss due to information theft was more than $350,000. A 2005 *InformationWeek*/Accenture survey of 2540 companies found that 78 percent of those companies believed that they were more vulnerable because the attackers were getting more sophisticated.

Online Warfare and Terrorism

Many Internet security experts believe that we are at the dawn of a new age of terrorism and warfare that could be carried out or coordinated through the Internet. A considerable number of Web sites currently exist that openly support or are operated by hate groups and terrorist organizations. Web sites that contain detailed instructions for creating biological weapons and other poisons, discussion boards that help terrorist groups recruit new members online, and sites that offer downloadable terrorist training films now number in the thousands.

The Internet provides an effective communications network on which many people and businesses have become dependent. Although the Internet was designed from its inception to continue operating while under attack, a sustained effort by a well-financed terrorist group or rogue state could slow down the operation of major transaction-processing centers. As more business communications traffic moves to the Internet, the potential damage that could result from this type of attack increases. You will learn more about security threats and countermeasures for those threats in Chapter 10.

ETHICAL ISSUES

Companies using Web sites to conduct electronic commerce should adhere to the same ethical standards that other businesses follow. If they do not, they will suffer the same consequences that all companies suffer: the damaged reputation and long-term loss of trust that can result in loss of business. In general, advertising or promotion on the Web should include only true statements and should not omit any information that could mislead potential purchasers or wrongly influence their impressions of a product or service. Even true statements have been held to be misleading when the ad omits important related facts. Any comparisons to other products should be supported by verifiable information. The next section explains the role of ethics in formulating Web business policies, such as those affecting visitors' privacy rights and companies' Internet communications with children.

Ethics and Web Business Policies

Web businesses are finding that ethical issues are important to consider when they are making policy decisions. Recall from Chapter 3 that buyers on the Web often communicate with each other. A report of an ethical lapse that is rapidly passed among customers can seriously affect a company's reputation. In 1999, *The New York Times* ran a story that disclosed Amazon.com's arrangements with publishers for book promotions. Amazon.com was accepting payments of up to $10,000 from publishers to give their books editorial reviews and placement on lists of recommended books as part of a cooperative advertising program. When this news broke, Amazon.com issued a statement that it had done nothing wrong and that such advertising programs were a standard part of publisher-bookstore relationships. The outcry on the Internet in newsgroups and mailing lists was overwhelming. Two days later—before most mass media outlets had even reported the story—Amazon.com announced that it would end the practice and offer unconditional refunds to any customers who had purchased a promoted book. Amazon.com had done nothing illegal, but the practice appeared to be unethical to many of its existing and potential customers.

In early 1999, eBay faced a similar ethical dilemma. Several newspapers had begun running stories about sales of illegal items, such as assault weapons and drugs, on the eBay auction site. At this point in time, eBay was listing about 250,000 items each day. Although eBay would investigate claims that illegal items were up for auction on its site, eBay did not actively screen or filter listings before the auctions were placed on the site.

Even though eBay was not legally obligated to screen the items auctioned, and even though screening would be fairly expensive, eBay's executive team decided that screening for illegal and copyright-infringing items would be in the best long-run interest of eBay. The team decided that such a decision would send a signal about the character of the company to its customers and the public in general. The eBay executive team also decided to remove an entire category—firearms—from the site. Not all of eBay's users were happy about this decision—the sale of firearms on eBay, when done properly, was legal. However, the eBay executive team again decided that presenting an overall image of an open and honest marketplace was so important to the future success of eBay that it chose to ban all firearms sales.

An important ethical issue that organizations face when they collect e-mail addresses from site visitors is how the organization limits the use of the e-mail addresses and related information. In the early days of the Web, few organizations made any promises to visitors who provided such information. Today, most organizations state their policy on the protection of visitor information, but many do not. In the United States, organizations are not legally bound to limit their use of information collected through their Web sites. They may use the information for any purpose, including the sale of that information to other organizations. This lack of government regulation that might protect site visitor information is a source of concern for many individuals and privacy rights advocates. These concerns are discussed in the next section.

Privacy Rights and Obligations

The issue of online privacy is continuing to evolve as the Internet and the Web grow in importance as tools of communication and commerce. Many legal and privacy issues remain

unsettled and are hotly debated in various forums. The **Electronic Communications Privacy Act of 1986** is the main law governing privacy on the Internet today. Of course, this law was enacted before the general public began its wide use of the Internet. The law was written to update existing law that prevented interception of audio signal transmissions so that any type of electronic transmissions (including, for example, fax or data transmissions) would be given the same protections. In 1986, the Internet was not used to transmit commercially valuable data in any significant amount, so the law was written to deal primarily with interceptions that might occur on leased telephone lines.

In recent years, a number of legislative proposals have been advanced that specifically address online privacy issues, but, thus far, none have withstood constitutional challenges. In July 1999, the FTC issued a report that examined how well Web sites were respecting visitors' privacy rights. Although it found a significant number of sites without posted privacy policies, the report concluded that companies operating Web sites were developing privacy practices with sufficient speed and that no federal laws regarding privacy were required at that time. Privacy advocacy groups responded to the FTC report with outrage and calls for legislation. Thus, the near-term future of privacy regulation in the United States is unclear. The Direct Marketing Association (DMA), a trade association of businesses that advertise their products and services directly to consumers using mail, telephone, Internet, and mass media outlets, has established a set of privacy standards for its members. However, critics note that past efforts by the DMA to regulate its members' activities have been less than successful.

Ethics issues are significant in the area of online privacy because laws have not kept pace with the growth of the Internet and the Web. The nature and degree of personal information that Web sites can record when collecting information about visitors' page-viewing habits, product selections, and demographic information can threaten the privacy rights of those visitors. This is especially true when companies lose control of the data they collect on their customers (and other people). In recent years, many companies have made news headlines because they allowed confidential information about individuals to be released without the permission of those individuals. ChoicePoint (a company that compiles information about consumers) sold the names, addresses, Social Security numbers, and credit reports of more than 145,000 people to thieves who posed as legitimate businesses. More than 1000 fraud cases have been documented as a result of that privacy violation. Hackers broke into customer databases at DSW Shoe Warehouse and stole the credit card numbers, checking account numbers, and driver's license numbers of more than 1.4 million customers. In another hacking case, a computer at Boston College was penetrated and the addresses and Social Security numbers of 120,000 alumni were exposed. But not all privacy compromises are the work of external agents. Sometimes, companies just lose things. In 2005, Ameritrade, Bank of America, and Time Warner each reported that they had lost track of shipments containing computer backup tapes that held confidential information for hundreds of thousands of customers or employees.

The Internet has also changed traditional assumptions about privacy because it allows people anywhere in the world to gather data online in quantities that would have been impossible a few years ago. For example, real estate transactions are a matter of public record in the United States. These transactions have been recorded in county records for many years and have been available to anyone who wanted to go to the county recorder's office and spend hours leafing through large books full of handwritten records. Many counties have made these

records available on the Internet, so now a researcher can examine thousands of real estate transaction records in hours without traveling to a single county office. Many privacy experts see this change in the ease of data access to be an important shift that affects the privacy rights of those who participate in real estate transactions. Because the Internet makes such data more readily available to a wider range of people, the privacy previously afforded to the participants in those transactions has been reduced.

Differences in cultures throughout the world have resulted in different expectations about privacy in electronic commerce. In Europe, for example, most people expect that information they provide to a commercial Web site will be used only for the purpose for which it was collected. Many European countries have laws that prohibit companies from exchanging consumer data without the express consent of the consumer. In 1998, the European Union adopted a Directive on the Protection of Personal Data. This directive codifies the constitutional rights to privacy that exist in most European countries and applies them to all Internet activities. In addition, the directive prevents businesses from exporting personal data outside the European Union unless the data will continue to be protected in accordance with provisions of the directive. The European Union and its member countries have consistently exhibited a strong preference for using government regulations to protect privacy. The United States has exhibited an opposite preference. U.S. companies, especially those in the direct mail marketing industry, have consistently and successfully lobbied to avoid government regulation and allow the companies to police themselves.

One of the major privacy controversies in the United States today is the opt-in vs. opt-out issue. Most companies that gather personal information in the course of doing business on the Web would like to be able to use that information for any purpose of their own. Some companies would also like to be able to sell or rent that information to other companies. No U.S. law currently places limits on companies' use of such information. Companies are, in general, also free to sell or rent customer information. An increasing number of U.S. companies do provide a way for customers who would like to restrict use of their personal information to do so. The most common policy used in U.S. companies today is an opt-out approach. In an **opt-out** approach, the company collecting the information assumes that the customer does not object to the company's use of the information unless the customer specifically chooses to deny permission (that is, to opt out of having their information used). In the less common **opt-in** approach, the company collecting the information does not use the information for any other purpose (or sell or rent the information) unless the customer specifically chooses to allow that use (that is, to opt in and grant permission for the use). Figure 7-6 (on the next page) shows an example Web page that presents a series of opt-in choices to site visitors. The Web site will not send any of these three items to a site visitor unless that visitor opts in by checking one or more boxes.

Figure 7-7 shows the opt-out approach. A Web site that uses the opt-out approach will send all three items to the site visitor unless the site visitor checks the boxes to indicate that the items are not wanted.

As you can see, it is easy for site visitors to misread the text and make the wrong choice when deciding whether or not to check the boxes. Sites that use the opt-out approach are often criticized for requiring their visitors to take an affirmative action (checking the empty boxes) to prevent the site from sending items. Another approach to presenting opt-out choices is to use a page that includes checked boxes and instructs the visitor to "uncheck the boxes of the items you do not wish to receive." Most privacy advocates believe

FIGURE 7-6 Sample Web page showing opt-in choices

FIGURE 7-7 Sample Web page showing opt-out choices

that the opt-in approach is preferable because it gives the customer privacy protection unless that customer specifically elects to give up those rights. Most U.S. businesses have traditionally taken the position that they have a right to use the information they collect unless the provider of the information explicitly objects. Some of these companies are changing to the opt-in approach, often at the prodding of privacy advocacy groups.

Until the legal environment of privacy regulation becomes more clear, privacy advocates recommend that electronic commerce Web sites be conservative in their collection and use of customer data. Mark Van Name and Bill Catchings, writing in *PC Week* in 1998, outlined four principles for handling customer data that provide a good outline for Web site administrators even today. These principles are as follows:

- Use the data collected to provide improved customer service.
- Do not share customer data with others outside your company without the customer's permission.
- Tell customers what data you are collecting and what you are doing with it.
- Give customers the right to have you delete any of the data you have collected about them.

Today, we might add to this list a recommendation that customer data, once collected, be kept as secure as possible. A number of organizations are active in promoting privacy rights. You can learn more about current developments in privacy legislation and practices throughout the world by following the links to these organizations' Web sites that appear under the heading **Privacy Rights Advocacy Groups** in the Online Companion.

LEARNING FROM FAILURES

DOUBLECLICK

As you learned in Chapter 4, **DoubleClick** is one of the largest banner advertising networks in the world. DoubleClick arranges the placement of banner ads on Web sites. Like many other Web sites, DoubleClick uses **cookies**, which are small text files placed on Web client computers, to identify returning visitors.

Most visitors find the privacy risk posed by cookies to be acceptable. Visitors to Amazon.com, for example, have Amazon.com cookies placed on their computers so that the Web server at Amazon.com recognizes them when they return. This can be useful, for example, when a visitor who has placed several items in a shopping cart before being interrupted can return to Amazon.com later in the day and find the shopping cart intact—the Web server can read the client's Amazon.com cookie and find the shopping cart from the client's previous session. The Amazon.com server can read only its own cookies; it cannot read the cookies placed on the client computer by any other Web server.

There are two important differences between the Amazon.com scenario and what happens when DoubleClick serves a banner ad. First, the visitor usually does not know that the banner ad is coming from DoubleClick (and thus, does not know that the DoubleClick server could be writing a cookie to the client computer). Second, DoubleClick serves ads through Web sites owned by thousands of companies. As a visitor moves from one Web site to another, that visitor's computer can collect many DoubleClick cookies. The DoubleClick server can read all of its own cookies, gathering information from each one about which ads were served and the sites through which they were served. Thus, DoubleClick can compile a tremendous amount of information about where a visitor has been on the Web.

Even this amount of information collection would not trouble most people. DoubleClick can use the cookies to track a particular computer's connections to Web sites, but it does not record any identity information about the owner of that computer. Therefore, DoubleClick accumulates a considerable record of Web activity, but cannot connect that activity with a person.

In 1999, DoubleClick arranged a $1.7 billion merger with Abacus Direct Corporation. Abacus had developed a way to link information about people's Web behavior (collected through cookies such as those placed by DoubleClick's banner ad servers) to the names, addresses, and other information about those people that had been collected in an offline consumer database.

The reaction from online privacy protection groups was immediate and substantial. The FTC launched an investigation, the Internet's privacy issues e-mail lists and chat rooms buzzed with discussions, and, in the end, DoubleClick abandoned its plans to integrate its cookie-generated data with the identity information in the Abacus database. Although DoubleClick is still one of the largest banner advertising networks, it has not met its profitability targets. DoubleClick had been counting on generating additional revenue by using the information in the combined database that it was unable to create.

When the FTC probe concluded two years later, DoubleClick was not charged with any violations of laws or regulations. The lesson here is that a company violates the Internet community's ethical standards at its own peril, even if the transgression does not break any laws.

Communications with Children

An additional set of privacy considerations arises when Web sites attract children and engage in some form of communication with those children. Adults who interact with Web sites can read privacy statements and make informed decisions about whether to communicate personal information to the site. The communication of private information (such as credit card numbers, shipping addresses, and so on) is a key element in the conduct of electronic commerce.

The laws of most countries and most sets of ethics consider children to be less capable than adults in evaluating information sharing and transaction risks. Thus, we have laws in the physical world that prevent or limit children's ability to sign contracts, get married, drive motor vehicles, and enter certain physical spaces (such as bars, casinos, tattoo parlors, and race tracks). Children are considered to be less able (or unable) to make informed decisions about the risks of certain activities. Similarly, many people are concerned about children's ability to read and evaluate privacy statements and then consent to providing personal information to Web sites.

Under the laws of most countries, people under the age of 18 or 21 are not considered adults. However, those countries that have proposed or passed laws that specify differential treatment for the privacy rights of children often define "child" as a person below the age of 12 or 13. This complicates the issue because it creates two classes of nonadults.

In the United States, Congress enacted the Children's Online Protection Act (COPA) in 1998 to protect children from "material harmful to minors." This law was held to be unconstitutional because it unnecessarily restricted access to a substantial amount of material that is lawful, thus violating the First Amendment. Congress was more successful with the **Children's Online Privacy Protection Act of 1998 (COPPA)**, which provides restrictions on data collection that must be followed by electronic commerce sites aimed at children. This law does not regulate content, as COPA attempted to do, so it has not been successfully challenged on First Amendment grounds. In 2001, Congress enacted the Children's Internet Protection Act (CIPA). The CIPA requires schools that receive federal funds to install filtering software on computers in their classrooms and libraries. Filtering software is used to block access to adult content Web sites. In 2003, the Supreme Court held that the CIPA was constitutional.

Companies with Web sites that appeal to nonadults must be careful to comply with the laws governing their interactions with these young visitors. **Disney Online** is a site that appeals primarily to young children. The Disney Online registration page offers three choices to visitors who want to register with the site and receive regular communications and updates. The first registration choice is for adults, a second choice is for "teens," and a third choice is for "kids." The "kids" choice leads to a screen that asks for a parent's e-mail address so that Disney can invite the parent to set up a family account. The Disney.com registration page for "teens" asks for the visitor's name, birthday, and the e-mail address of a parent. Disney uses the birthday to calculate the visitor's age and, if the age is less than 13, Disney uses the parent's e-mail address to notify parents of their child's registration and to invite them to set up a family account. Family accounts are controlled by parents who can elect to allow family members who are under the age of 13 to use the site. By refusing to enroll any child under age 13 as a site subscriber, Disney Online meets the requirements of the COPPA law. Other sites that appeal to a young audience use

similar techniques to limit unsupervised access to their Web pages. For example, Sanrio (the company that produces Hello Kitty and related products) asks for a birthdate before allowing access to its English-language site that is directed at U.S. customers, **Sanriotown**. As shown in Figure 7-8, the site encourages visitors to notify the company that operates the site if they know a child who has gained access to the site in violation of COPPA.

FIGURE 7-8 Sanrio's approach to COPPA compliance

TAXATION AND ELECTRONIC COMMERCE

Companies that do business on the Web are subject to the same taxes as any other company. However, even the smallest Web business can become instantly subject to taxes in many states and countries because of the Internet's worldwide scope. Traditional businesses may operate in one location and be subject to only one set of tax laws for years. By the time those businesses are operating in multiple states or countries, they have developed the internal staff and record-keeping infrastructure needed to comply with multiple tax laws. Firms that engage in electronic commerce must comply with these multiple tax laws from their first day of existence.

An online business can become subject to several types of taxes, including income taxes, transaction taxes, and property taxes. **Income taxes** are levied by national, state, and local governments on the net income generated by business activities. **Transaction taxes**, which include sales taxes, use taxes, excise taxes, and customs duties, are levied on the products or services that the company sells or uses. Customs duties are taxes levied by the United States and other countries on certain commodities when they are imported into the country. **Property taxes** are levied by states and local governments on the personal property and real estate used in the business. In general, the taxes that cause the greatest concern for Web businesses are income taxes and sales taxes.

Nexus

A government acquires the power to tax a business when that business establishes a connection with the area controlled by the government. For example, a business that is located in Kansas has a connection with the state of Kansas and is subject to Kansas taxes. If that company opens a branch office in Arizona, it forms a connection with Arizona and becomes subject to Arizona taxes on the portion of its business that occurs in Arizona. This connection between a taxpaying entity and a government is called **nexus**. The concept of nexus is similar in many ways to the concept of personal jurisdiction discussed earlier in this chapter. The activities that create nexus in the United States are determined by state law and thus vary from state to state. Nexus issues have been frequently litigated, and the resulting common law is fairly complex. Determining nexus can be difficult when a company conducts only a few activities in or has minimal contact with the state. In such cases, it is advisable for the company to obtain the services of a professional tax advisor.

Companies that do business in more than one country face national nexus issues. If a company undertakes sufficient activities in a particular country, it establishes nexus with that country and becomes liable for filing tax returns in that country. The laws and regulations that determine national nexus are different in each country. Again, companies will find the services of a professional tax lawyer or accountant who has experience in international taxation to be valuable.

U.S. Income Taxes

The **Internal Revenue Service (IRS)** is the U.S. government agency charged with administering the country's tax laws. A basic principle of the U.S. tax system is that any verifiable increase in a company's wealth is subject to federal taxation. Thus, any company whose U.S.-based Web site generates income is subject to U.S. federal income tax. Furthermore, a Web site maintained by a company in the United States must pay federal income tax on income generated outside of the United States. To reduce the incidence of double taxation of foreign earnings, U.S. tax law provides a credit for taxes paid to foreign countries. The IRS Web site's home page appears in Figure 7-9.

The IRS site includes links to downloadable tax forms, copies of IRS publications, current tax news, and other useful tax information. The home page offers links to sections of the Web site that are designed to help specific categories of site visitors.

Most states levy an income tax on business earnings. If a company conducts activities in several states, it must file tax returns in all of those states and apportion its earnings in accordance with each state's tax laws. In some states, the individual cities, counties, and other political subdivisions within the state also have the power to levy income taxes on business earnings. Companies that do business in multiple local jurisdictions must apportion their income and file tax returns in each locality that levies an income tax. The number of taxing authorities (which includes states, counties, cities, towns, school districts, water districts, and many other governmental units) in the United States exceeds 30,000.

Companies that sell through their Web sites do not, in general, establish nexus everywhere their goods are delivered to customers. Usually, a company can accept orders and ship from one state to many other states and avoid nexus by using a contract carrier such as FedEx or United Parcel Service to deliver goods to customers.

FIGURE 7-9 Internal Revenue Service home page

U.S. State Sales Taxes

Most states levy a transaction tax on goods sold to consumers. This tax is usually called a sales tax. Businesses that establish nexus with a state must file sales tax returns and remit the sales tax they collect from their customers. If a business ships goods to customers in other states, it is not required to collect sales tax from those customers unless the business has established nexus with the customer's state. However, the customer in this situation is liable for payment of a use tax in the amount that the business would have collected as sales tax if it had been a local business.

A **use tax** is a tax levied by a state on property used in that state that was not purchased in that state. Most states' use tax rates are identical to their sales tax rates. In addition to property purchased in another state, use taxes are assessed on property that is not "purchased" at all. For example, lease payments on vehicles are subject to use taxes in most states. The leased vehicle is not purchased (in any state) but when it is used in the lessee's state, it incurs that state's use tax. In the past, few consumers filed use tax returns and few states enforced their use tax laws with regularity. However, an increasing number of states are providing a line on their individual income tax returns that asks people to report and pay their use tax for the year along with their state income taxes. Some states allow taxpayers to estimate their use tax liability; others require an exact statement of the use tax amount.

Larger businesses use complex software to manage their sales tax obligations. Not only are the sales tax rates different in the 7500 U.S. sales tax jurisdictions (which include states, counties, cities, and other sales tax authorities), but the rules about which items are taxable differ. For example, New York's sales tax law provides that large marshmallows are taxable (because they are "snacks"), but small marshmallows are not taxable (because they are "food").

Some purchasers are exempt from sales tax, such as certain charitable organizations and businesses buying items for resale. Thus, to determine whether a particular item is subject to sales tax, a seller must know where the customer is located, what the laws of that jurisdiction say about taxability and tax rate, and the taxable status of the customer.

The sales tax collection process in the United States is largely regarded as a serious problem. Even the Supreme Court, in one of its sales tax decisions more than 10 years ago, stated that the situation is needlessly confusing and encouraged Congress to act. Although a number of bills have been introduced over the years, none has become law. Some large online retailers, such as Amazon.com, have announced that they will begin collecting and remitting sales tax on all sales, even when the sale is delivered into a state with which the company does not have nexus.

Many of the states have joined together through the **National Governor's Association** and the **National Conference of State Legislatures** to create the Streamlined Sales and Use Tax Agreement (SSUTA). The SSUTA simplifies state sales taxes by making the various state tax codes more congruent with each other while allowing each state to set its own rates. Each state must adopt the agreement, and once a state does adopt it, companies in the state can choose one of several simple procedures for collecting and remitting sales taxes nationwide.

European Union Value Added Taxes

The United States raises most of its revenue through income taxes. Other countries, especially those in the European Union (EU), use transfer taxes to generate most of their revenues. The Value Added Tax (VAT) is the most common transfer tax used in these countries. A VAT is assessed on the amount of value added at each stage of production. For example, if a computer keyboard manufacturer purchased keyboard components for $20 and then sold finished keyboards for $50, the value added would be $30. VAT is collected by the seller at each stage of the transaction. For example, a product that goes through five different companies on its way to the ultimate consumer would have VAT assessed on each of the five sales. In most countries, the VAT is calculated at the time of each intermediate sale and remitted to the country in which that sale occurs.

The EU enacted legislation concerning the application of VAT to sales of digital goods that became effective in mid-2003. Companies based in EU countries must collect VAT on digital goods no matter where in the EU the products are sold. This legislation has attracted the attention of companies based outside of the EU that sell digital goods to consumers based in one or more EU countries. Under the law, non-EU companies that sell into the EU must now register with EU tax authorities and levy, collect, and remit VAT if their sales include digital goods delivered into the EU.

Summary

The legal concept of jurisdiction on the Internet is still unclear and ill defined. The relationship between geographic boundaries and legal boundaries is based on four elements: power, effects, legitimacy, and notice. These four elements have helped governments create the legal concept of jurisdiction in the physical world. Because the four elements exist in somewhat different forms on the Internet, the jurisdiction rules that work so well in the physical world do not always work well in the online world.

As in traditional commerce, contracts are a part of doing business on the Web and are established through various types of offers and acceptances. Any contract for the electronic sale of goods or services includes implied warranties. Many companies include contracts or rules on their Web sites in the form of terms of service agreements. Contracts can be invalidated when one of the parties to the transaction is an imposter; however, forged identities are becoming easier to detect through electronic security tools.

Seemingly innocent inclusion of photographs, whether manipulated or not, and other elements on a Web page can lead to infringement of trademarks, copyrights, or patents; defamation; and violation of intellectual property rights. An international administrative mechanism now exists for resolving domain name disputes that has reduced the need for lengthy and expensive litigation in many cases. Electronic commerce sites must be careful not to imply relationships that do not actually exist. Negative evaluative statements about entities, even when true, are best avoided given the subjective nature of defamation and product disparagement.

Unfortunately, some people use the Internet for perpetrating crimes, advocating terrorism, and even waging war. Law enforcement agencies have found it difficult to combat many types of online crime, and governments are working to create adequate defenses for online war and terrorism.

Web business practices such as collecting information and tracking consumer habits have led to questions of ethics regarding online privacy. Some countries are far more restrictive than others in terms of what type of information collection is acceptable and legal. Companies that collect personal information can use an opt-in policy, in which the customer must take an action to permit information collection, or an opt-out policy, in which the customer must take an action to prevent information collection. Opt-in policies are more protective of customers' privacy rights. Web businesses also must be careful when communicating with children. In general, laws require parental consent be obtained before information is collected from children under the age of 13.

Companies that conduct electronic commerce are subject to the same laws and taxes as other companies, but the nature of doing business on the Web can expose companies to a large number of laws and taxes sooner than traditional companies usually face them. The international nature of all online business further complicates a firm's tax obligations. Although some legal issues are straightforward, others are difficult to interpret and follow because of the newness of electronic commerce and the unsettled nature of applicable law. The large number of government agencies that have jurisdiction and the power to tax makes it essential that companies doing business on the Web understand the potential liabilities of doing business with customers in those jurisdictions.

Key Terms

Acceptance
Authority to bind
Breach of contract
Business process patent
Common law
Consideration
Constructive notice
Contract
Cookies
Conflict of laws
Copy control
Copyright
Cybersquatting
Defamatory
Digital watermark
Domain name ownership change
Effects
Fair use
Forum selection clause
Implied contract
Income tax
Intellectual property
Judicial comity
Jurisdiction
Legitimacy
Long-arm statute
Name changing
Name stealing
Nexus
Notice
Offer
Opt-in
Opt-out
Patent
Per se defamation
Personal jurisdiction
Power
Product disparagement
Property tax
Service mark
Signature
Statute of Frauds
Statutory law
Subject-matter jurisdiction
Terms of service (ToS)
Tort
Trade name
Trademark
Trademark dilution
Transaction tax
Use tax
Vicarious copyright infringement
Warranty disclaimer
Writing

Review Questions

RQ1. In about 100 words, explain why online businesses might have difficulty limiting the effects of their actions to a relatively small geographic area.

RQ2. In about 300 words, describe the differences between subject-matter jurisdiction and personal jurisdiction.

RQ3. The advantages and disadvantages of issuing business process patents have been hotly debated by legal scholars and business people. One compromise proposal advanced by Jeff Bezos, founder of Amazon.com, is to allow the issuance of business patents, but only allow them to be effective for a short time, perhaps two or three years. In about 300 words,

present logical and factual arguments that support the issuance of such limited-term business process patents.

RQ4. Define product disparagement. In two or three paragraphs, present an example of product disparagement.

RQ5. In about 300 words, explain the idea of nexus. Why is it an important concept in state and international taxation? In what ways is it similar to jurisdiction?

Exercises

E1. Use **Google** or your favorite Web search engine to obtain a list of Web pages that include the words "privacy statement." Visit the Web pages on the search results list until you find a page that includes the text of a privacy statement. Print the page and turn it in with your answers to the following questions:

- Does the site follow an opt-in or opt-out policy (or is the policy not clearly stated in the privacy statement)?
- Does the privacy statement include a specific provision or provisions regarding the collection of information from children?
- Does the privacy statement describe what happens to the collected personal information if the company goes out of business or is sold to another company? List those provisions.

Write one paragraph in which you evaluate the clarity of the privacy statement.

E2. Use your favorite search engine, the links in the Online Companion for this exercise, and your library to learn more about the Napster lawsuit. Identify the main issues in the case and the principal arguments that could be used by either side.

- In about 300 words, present the case against Napster.
- In about 300 words, present one or more well-reasoned arguments to support Napster's position.

E3. Use **Google** or your favorite search engine to find a Web site (other than Disney or Sanriotown) that is directed to young people. Examine the site to determine how it complies with COPPA. Test the site to ensure that it does not accept information from children under the age of 13. Evaluate the site's compliance with COPPA in a report of about 200 words.

E4. In the United States, a law called the Internet Tax Moratorium (ITM) has been enacted and renewed several times. The purpose of the ITM is to prevent federal, state, or local governments from enacting any new taxes on Internet business activities. Use **Google** or your favorite search engine to learn more about the ITM. In about 300 words, critically evaluate the rationale behind the law and take a position on whether the law should be renewed again.

Cases

C1. Nissan.com

The Nissan Motor Company of Japan had sold its cars in the United States under the brand name Datsun for many years. In the late 1980s, the company changed its branding policy and began selling cars in the U.S. market with the name of Nissan. However, the company did not realize that

the Web would become an important marketing tool and did not register the name nissan.com as soon as it became available.

Nissan was not the only auto company to miss an opportunity to register its brand's domain name early. General Motors had registered the domain gm.com in 1992, but it had not registered generalmotors.com. The company had to purchase that name from Gil Vanorder, who had registered it in 1997. Vanorder's site featured a cigar-smoking, uniform-wearing cartoon character named "General John C. Motors." Volkswagen (which had registered vw.com when it first became available) successfully sued Virtual Works (an ISP) to obtain the domain name vw.net. Other auto companies have purchased or sued (with mixed results) to obtain domain names that included their product brand names. DaimlerChrysler was able to purchase dodge.com in 2001 from the London financial software company that had registered it originally. Ford had to sue National A-1 Advertising to obtain the right to use lincoln.com. However, Ford was unsuccessful in its attempts to obtain mercury.com. That name is still used by the New York City information technology services company, Mercury Technologies, that first registered the name.

In 1991, Uzi Nissan formed a company named Nissan Computer Corp. in North Carolina to sell computer hardware and provide related repair and consulting services. Nissan's company also offered networking hardware for sale, along with related services. In 1994, the company registered the name nissan.com. In 1996, the company registered the domain name nissan.net and began offering ISP services to individuals and companies at that Web site.

In 1995, he received a letter from a lawyer representing Nissan Motor Company. The letter requested information about how Nissan was planning to use the domain name nissan.com. Since he was operating a computer company and Nissan was an auto company, Nissan decided there would be no potential confusion in customers' minds about the relationship (or lack thereof) between Nissan Computer and Nissan Motors. Nissan did not respond to the letter. The lawyer did not follow up with any other contact, so Nissan considered the issue closed.

In 2000, Nissan Motors sued Nissan Computer under the U.S. Anticybersquatting Consumer Protection Act for $10 million and the exclusive right to use the names nissan.com and nissan.net. Uzi Nissan argued in court that he was just using his family name (which is a common name in the Middle East) to which he had a basic right, that he had no intent to profit from the name (he was unwilling to sell it to Nissan Motors at any price), and that there was little likelihood that his computer store would be confused in the minds of the consumers with the international auto company of the same name. Nissan Motors argued that its brand name was so well known that any alternative use of the name would be confusing to consumers.

In 2002, opinions issued by the California Superior Court and the U.S. Ninth Circuit District Court held that Nissan Computer had not acted in bad faith when it acquired the disputed domain names. However, the court ruled that Nissan Computer could no longer use the domain names for commercial purposes because of the potential confusion it could create in the minds of consumers. Nissan Computer would have to find a different domain name for its business. The court also ordered that Nissan could not place any advertising on his Web sites at nissan.com or nissan.net and prohibited him from placing disparaging remarks or negative commentary about Nissan Motors (or links to such remarks or commentary) on the two sites. The court did not, however, order the transfer of the two domain names to Nissan Motor. The Online Companion includes links to the Web sites operated today by Nissan Computer and Nissan Motors.

Required:

1. U.S. courts sometimes appoint advisors (often called Special Masters) to help them decide cases that involve complex business or technical issues. Assume you are a business advisor to a court that is hearing an appeal of the *Nissan Motor Co. v. Nissan Computer Corp.* case. In about 200 words, explain why Nissan Motors is so concerned about the use of these two domain names and how a monetary damages judgment of $10 million could be justified (if you do not believe that the monetary damages are justified, explain why).
2. In about 200 words, provide an outline of the ethics of the position taken by Uzi Nissan in this dispute.
3. In about 200 words, provide an outline of the ethics of the position taken by Nissan Motors in this dispute.
4. If you believe that the courts' decisions in this case are fair to the parties and the general public, explain why in about 200 words. If you believe that the courts' decisions are not fair, outline a decision (in about 200 words) that you believe would be fair.

Note: Your instructor might assign you to a group to complete this case, and might ask you to prepare a formal presentation of your results to your class.

C2. Ellasaurus Products Enterprises

Ellen Carson is the author and illustrator of a successful series of children's books that chronicle the adventures of Ellasaurus, a 4-year-old orange dinosaur. Ellen has done well with the books, but her business advisors have told her that she could earn considerably more money by creating a merchandising business around the Ellasaurus character. Following this advice, she has created Ellasaurus Products Enterprises (EPE), a company that has begun developing and marketing Ellasaurus toys, stuffed animals, coloring books, pajamas, and Halloween costumes.

EPE has had some success in its attempts to get major retailers to stock the Ellasaurus product line, but Ellen is concerned that retailers might not be willing to take on a new and unproven product. She would like to create a Web site through which EPE could sell its merchandise directly to customers. She also sees the Web site as a way to build customer loyalty. Ellen envisions a site with a number of portal features in addition to the product sales. For example, she would like to offer online games, chat rooms, e-mail accounts, and other activities that would promote EPE products and her books.

The Ellasaurus book series appeals to children that are between 4 and 6 years old. Ellen expects the EPE product line to appeal to children in about the same age range. Ellen has visited sites such as **Hello Kitty** and **Nick Jr.** , which appeal to similar age groups, to get ideas for the site. She would like the site to be appealing to her main audience, but she would like to obtain registration information from site visitors so EPE can send e-mails with information about new products and Web site features to them.

Ellen plans to limit the Web site's merchandise sales to U.S. residents at first, but she hopes to begin selling internationally within a few years. The site will allow visitors from any country to register and participate in the online portal features.

Required:

1. Ellen will use some copyrighted illustrations from her books on the Web site. She will also include themes from the story lines of her books in some of the games that will be available (free) on the site to registered visitors. Prepare a report of about 300 words in which you discuss at least two intellectual property issues that might arise in the operation of the Web site.
2. In about 200 words, describe the ethical issues that Ellen faces because of the ages of her intended audience members.
3. In about 300 words, outline the laws with which the site must comply when it registers site visitors under the age of 13. Include recommendations regarding how Ellen can best comply with those laws.
4. In about 300 words, describe the sales tax liabilities to which the Web site will be exposed. Assume that Ellen will operate the site from her home office in Michigan and that EPE will manufacture the merchandise in Texas. The merchandise will be warehoused at EPE distribution centers in New Jersey, Ohio, and California.

Note: Your instructor might assign you to a group to complete this case, and might ask you to prepare a formal presentation of your results to your class.

For Further Study and Research

Angwin, J. 2001. "Are Domain Panels the Hanging Judges of Cyberspace?" *The Wall Street Journal*, August 20, B1.

Angwin, J. and D. Bank. 2005. "Time Warner Alerts Staff to Lost Data: Files for 600,000 Workers Vanish During Truck Ride," *The Wall Street Journal*, May 3, A3.

Bagby, J. and F. McCarty. 2003. *The Legal and Regulatory Environment of E-Business.* Cincinnati: Thomson South-Western.

Bodeen, C. 2004. "China Shuts Down Internet Blogs," *Salon.com*, March 19. (http://www.salon.com/news/wire/2004/03/19/blogs2/index.html)

Brilmayer, L. 1989. "Consent, Contract, and Territory," *Minnesota Law Review*, 74(1), 11–12.

Cass, S. 2002. "Nissan v. Nissan," *IEEE Spectrum*, 39(10), October, 53–54.

Claburn, T., M. Garvey, and V. Koen. 2005. "The Threats Get Nastier," *InformationWeek*, August 29, 34–41.

Clark, P. 2001. "Doubts Cloud DoubleClick's Repositioning," *B to B*, 86(15), August 28, 1–2.

Coll, S. and S. Glasser. 2005. "Terrorists Turn to the Web as Base of Operations," *The Washington Post*, August 7, A1.

Cope, N. 2000. "A Hit for Jethro Tull in Domain Name Dispute," *The Independent*, July 31, 15.

Crane, E. 2000. "Double Trouble," *Ziff Davis Smart Business*, 13(10), October, 62.

Creed, A. 2001. "E-Trade Swallows $90,000 Fine," *BizReport*, July 10. (http://www.bizreport.com/ article.php?id=1692)

Digital Millennium Copyright Act. 1998. Public Law No. 105-304, 112 Statutes 2860.

Direct Marketing. 2001. "FTC Closes DoubleClick Investigation," 63(12), April, 18.

The Economist. 2000. "Business Ethics: Doing Well by Doing Good," 355(8167), April 22, 65–67.

The Economist. 2000. "The Internet's Chastened Child," 357(8196), November 11, 80.

Federal Trade Commission (FTC). 1999. *Self-Regulation and Privacy Online: A Report to Congress.* Washington: FTC.

Flynn, L. 2000. "Whose Name Is It Anyway? Arbitration Panels Favoring Trademark Holders in Disputes Over Web Names," *The New York Times*, September 4, C3.
Foege, A. 2005. "Extortion.com," *Fortune Small Business*, September 1. (http://www.fortune.com/fortune/print/0,15935,1092651,00.html)
Foster, A. 2002. "Computer Crime Incidents at Two California Colleges Tied to Investigation Into Russian Mafia," *Chronicle of Higher Education*, June 24. (http://chronicle.com/free/2002/06/2002062401t.htm)
Granholm v. Heald 544 US _____ (2005).
Greene, S. 2001. "Reconciling Napster with the Sony Decision and Recent Amendments to Copyright Law," *American Business Law Journal*, 39(1), Fall, 57–98.
Greenhouse, L. 2003. "Court Upholds Law to Make Libraries Use Internet Filters," *The New York Times*, June 24, A1.
Hamblen, M. 2003. "Regulatory Requirements Place New Burdens on IT: U.S. Firms Scramble to Comply with EU Tax," *Computerworld*, June 30, 1.
Hardesty, D. 2004. *Electronic Commerce Taxation and Planning, 2004 Update Edition*. Boston: Warren, Gorham & Lamont.
Hardesty, D. 2004. *Sales Tax and Electronic Commerce*. Larkspur, CA: ClickBank.
Harmon, A. 2001. "As Public Records Go Online, Some Say They're Too Public," *The New York Times*, August 24, A1.
Harvard Law Review. 1999. "The Criminalization of Copyright Infringement in the Digital Era," 112(7), May, 1705–1722.
Heckman, J. 2000. "Trademarks Protected Through New Cyber Act," *Marketing News*, 34(1), January 3, 6–7.
Hemphill, T. 2000. "DoubleClick and Consumer Online Privacy: An E-Commerce Lesson Learned," *Business & Society Review*, 105(3), Fall, 361–372.
Hirschman, C. 2001. "Prosecuting in the Name of Privacy," *Telephony*, 241(7), August 13, 82.
Hulme, G. 2005. "Extortion Online," *InformationWeek*, September 13, 24–25.
Hurt, E. 2000. "FTC Wins Internet's Respect," *Business 2.0*, October 13. (http://www.business2.com/content/ channels/technology/2000/10/13/21123)
Hutheesing, N. 2001. "Master of Your Domain," *Forbes*, 167(5), Spring, 60.
Hwang, W. and J. Klosek. 2003. "Taxing the Sale of Digital Goods in Europe," *E-Commerce Law & Strategy*, 20(3), July 11, 1.
Ian, J. 2002. "The Internet Debacle: An Alternative View," *Performing Songwriter Magazine*, May. (http://www.janisian.com/)
Isenberg, D. 2000. "Many Trademarks, But Just One Domain Name," *Internet World*, July 1, 86.
Jones, J. 2000. "Protecting Privacy," *InfoWorld*, 22(18), May 1, 40–41.
Journal of Internet Law. 2002. "Computer Firm's Use of Nissan.com Not Bad Faith Under Anticybersquatting Act," 6(1), July, 23.
Kahin, B. and C. Nesson (eds.). 1997. *Borders in Cyberspace*. Cambridge, MA: MIT Press.
Kaplan, C. 2002. "A Libel Suit May Decide E-Jurisdiction," *The New York Times*, May 27. (http://www.nytimes.com/2002/05/27/technology/27ELAW.html)
Keeler, D. 2000. "Taxation Slips Through the Net," *Global Finance*, 14(6), June, 60–61.
Kisiel, R. 2002. "Two Nissans Collide on Information Highway," *Automotive News*, December 16, 1IT–2IT.
Krim, J. 2004. "Justice Department to Announce Cyber-Crime Crackdown: Actions to Include Arrests, Subpoenas," *The Washington Post*, August 25, E5.

Leonard, A. 2002. "Nissan vs. Nissan," *Salon.com*, June 3. (http://www.salon.com/tech/col/leon/2002/06/03/ nissan/index.html)
Lessig, L. 2000. *Code and Other Laws of Cyberspace*. New York: Basic Books.
Liptak, A. 2003. "U.S. Courts' Role in Foreign Feuds Comes Under Fire," *The New York Times*, August 3, 1.
Manjoo, F. 2001. "Fine Print Not Necessarily in Ink," *Wired News*, April 6. (http://www.wired.com/news/business/0,1367,42858,00.html)
McClintock, M., N. Maguire, J. Kilby, and D. Barlow. 2000. "Electronic Commerce," *International Tax Review*, July-August, 9–13.
Meller, P. 2000. "Europe Passes Stiff E-Commerce Law," *The Industry Standard*, December 1. (http://www. thestandard.com/article/display/0,1151,20526,00.html)
Miller, R. and G. Jentz. 2002. *Law for E-Commerce*. Cincinnati: West.
Moran, J. and J. Kummer. 2003. "U.S. and International Taxation of the Internet: Part I," *Computer & Internet Lawyer*, 20(4), April, 1–18.
Mueller, M. 2002. *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy*. Syracuse, NY: Syracuse University Convergence Center. (http://dcc.syr.edu/roughjustice.htm)
Murray, J. 2000. "E-Contracts Present Courts with Special Legal Challenges," *Purchasing*, 129(3), August 24, 119-120.
Nee, E. 2005. "Days of Wine and Roses," *CIO Insight*, July, 25–26.
Network Briefing Daily. 2002. "Amazon Settles 1-Click Patent Dispute," March 8, 3–4.
Nigro, D. 2005. "Supreme Court Lifts Shipping Bans," *Wine Spectator*, 30(6), July 31, 12–12.
Nissan Motor Co. v. Nissan Computer Corp., 246 F.3d 675 (9th Cir. 2002).
O'Brien, T. 2005. "The Rise of the Digital Thugs," *The New York Times*, August 7, C1.
Oder, N. 2002. "COPA Ruling Offers Mixed Message," *Library Journal*, 127(11), June 15, 15.
Olavsrud, T. 2002. "Supreme Court Partially Lifts Bar on COPA ," *Internet News*, May 13. (http://www.internetnews.com/bus-news/article.php/1121271)
Olin, J. 2001. "Reducing International E-Commerce Taxes," *World Trade*, 14(3), March, 64–66.
Oliva, R. and S. Prabakar. 1999. "Copyright Perils Can Lurk on the Business Web," *Marketing Management*, 8(1), Spring, 54–57.
Pantazis, A. 1999. "Zeran v. America Online, Inc.: Insulating Internet Service Providers from Defamation Liability," *Wake Forest Law Review*, 34(2), Summer, 531–555.
Phillips, D. 2003. "JetBlue Apologizes for Use of Passenger Records," *The Washington Post*, September 20, E1.
Porter, K. and S. Bradley. 1999. *eBay, Inc.* Case #9-700-007. Cambridge, MA: Harvard Business School.
Radcliff, D. 2000. "Domain Name Game," *Computerworld*, 34(24), June 12, 71.
Reagle, J. 1999. "The Platform for Privacy Preferences," *Communications of the ACM*, 42(2), February, 48–51.
Rewick, J. 2000. "DoubleClick Finds Its Abacus Unit Nettlesome," *The Wall Street Journal*, October 19, B6.
Richtel, M. 2004. "U.S. Steps Up Push Against Online Casinos by Seizing Cash," *The New York Times*, May 31, C1.
Samborn, H. 2000. "Nibbling Away at Privacy," *ABA Journal*, 86(2), June, 26-27.
Samuelson, P. 1999. "Good News and Bad News on the Intellectual Property Front," *Communications of the ACM*, 42(3), March, 19–24.

Shaller, D. 2000. "E-mail, the Internet, and Other Legal and Ethical Nightmares," *Strategic Finance*, August, 82(2), 48–52.
Smedinghoff, T. (ed.). 1996. *Online Law: The SPA's Legal Guide to Doing Business on the Internet*. Reading, MA: Addison-Wesley Developers Press.
Stellin, S. 2002. "In Fights Over .Com Names, Trademark Owners Usually Win," *The New York Times*, June 24, 4.
Stone, M. 2001. "Court Dismisses Class Action Against eBay," *BizReport*, January 19. (http://www.bizreport.com/ daily/2001/01/20010119-4.htm)
Surowiecki, J. 2003. "Patent Bending," *The New Yorker*, July 14, 36.
Swire, P. and R. Litan. 1998. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington: Brookings Institution Press.
Tanford, J. 2005. "*Granholm v. Heald*: The Supreme Court Strikes Down Trade Barriers Against the Direct Sale of Wine," *Duke Law School: Supreme Court Online*, May. (http://www.law.duke.edu/publiclaw/supremecourtonline/commentary/gravhea.html)
Tynan, D. 2000. "Privacy 2000: In Web We Trust?" *PC World*, 18(6), June, 103–111.
United Nations. 1970. "Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations," *General Assembly Resolution*, #2625, 35th Session.
Van Name, M. and B. Catchings. 1998. "Practical Advice About Privacy and Customer Data," *PC Week*, 15(27), July 6, 38.
Warner, M. 2002. "The New Napsters," *Fortune*, 146(3), August 12, 115–116.
Wiley, L. 1999. "Proposed Revisions to European Copyright Laws Cause a Stir," *E Media Professional*, 12(4), April, 16–17.
Wilke, J. 2001. "Twenty States Oppose Airlines' Proposal for Joint Venture in Online Reservations," *The Wall Street Journal*, January 11, A10.
Whitlock, C. 2005. "Briton Used Internet As His Bully Pulpit," *The Washington Post*, August 8, A1.
Wingfield, N. 2002. "Napster Boy, Interrupted: Shawn Fanning Discusses Demise of His Brainchild And Future of Online Music," *The Wall Street Journal*, October 1, B1.
Wood, C. 2001. "Collusion in the Air," *PC Magazine*, 20(9), May 8, 199.