|  |
| --- |
| Chapter 7 |
|  |

**Internet Law,**

**Social Media, and Privacy**

**Introduction**

A start-up software company finds that there are others who have similar business and domain names. What options do they have for resolving the conflict? The protection of intellectual prop­erty relating to computers posed difficulties for courts because the legislators who drafted patent, trademark, and copy­right laws did not envision digital technol­ogy. Previous laws have also had to be amended, or new laws created, to protect these rights in the online world.

This chapter provides an overview of the principles that guide these amended laws and new legislation, as well as developments in the world of social media and the sphere of privacy. These topics concern all businesses—every employer and employee, chief executive officer and shareholder, customer and supplier, and consumer and critic. Part of doing business is being aware of the changes in these fields.

**Chapter Outline**

**I. Internet Law**

Unsolicited e-mail, domain names, and cybersquatting are among issues that arise only on the Internet.

**A. Spam**

Spam is junk e-mail.

**1. State Regulation of Spam**

Most states regulate spam. Many of these require the senders to tell recipients how to opt out of future mailings. Increasingly, states are passing laws to prohibit spam.

**2. The Federal CAN-SPAM Act**

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act preempts state anti-spam statutes, ex­cept for those that prohibit deceptive e-mailing practices, and permits the use of unsolicited commer­cial e-mail but prohibits certain spamming activities, including—

• The use of false return addresses and other misleading or deceptive information.

• “Dictionary attacks”—sending messages to randomly generated e-mail addresses.

• “Harvesting” e-mail addresses from Web sites.

|  |
| --- |
| **Additional Background—** |
|  |
| **Spam** |
|  |
| Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act in 2003 to take effect in 2004. The act applies to “commercial electronic mail messages” that are sent to promote a product or service. Unsolicited commercial e-mail is allowed under the act, but its use is regulated to prohibit false, deceptive, or misleading information and to limit the spread of unwanted **spam**. Following is part of the text of the CAN-SPAM Act. |
|  |
| **18 U.S.C. Section 1037** |
|  |
| **Fraud and related activity in connection with electronic mail** |
|  |
| **(a) In general.**—Whoever, in or affecting interstate or foreign commerce, knowingly— |
|  |
| **(1)** accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer, |
|  |
| **(2)** uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages, |
|  |
| **(3)** materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages, |
|  |
| **(4)** registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or |
|  |
| **(5)** falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses, or conspires to do so, shall be punished as provided in subsection (b). |
|  |
| **(b) Penalties.**—The punishment for an offense under subsection (a) is— |
|  |
| **(1)** a fine under this title, imprisonment for not more than 5 years, or both, if— |
|  |
| **(A)** the offense is committed in furtherance of any felony under the laws of the United States or of any State; or |
|  |
| **(B)** the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system; |
|  |
| **(2)** a fine under this title, imprisonment for not more than 3 years, or both, if— |
|  |
| **(A)** the offense is an offense under subsection (a)(1); |
|  |
| **(B)** the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations; |
|  |
| **(C)** the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period; |
|  |
| **(D)** the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period; |
|  |
| **(E)** as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or |
|  |
| **(F)** the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and |
|  |
| **(3)** a fine under this title or imprisonment for not more than 1 year, or both, in any other case. |
|  |
| **(c) Forfeiture.**— |
|  |
| **(1) In general.**—The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States— |
|  |
| **(A)** any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and |
|  |
| **(B)** any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense. |
|  |
| **(2) Procedures.**—The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 or the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section. |
|  |
| **(d) Definitions.**—In this section: |
|  |
| **(1) Loss.**—The term “loss” has the meaning given that term in section 1030(e) of this title. |
|  |
| **(2) Materially.**—For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation. |
|  |
| **(3) Multiple.**—The term “multiple” means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period. |
|  |
| **(4) Other terms.**—Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003 [15 U.S.C. Section 7701]. |
|  |

**3. The U.S. Safe Web Act**

• The Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond the Borders (U.S. Safe Web) Act of 2006 allows the Federal Trade Commission (FTC) to cooperate and share information with foreign agencies investigating and prosecuting Internet fraud, spamming, and spyware.

• Internet service providers (ISPs) have a “safe harbor”—immunity from liability—for supplying information to the FTC concerning unfair or deceptive conduct in foreign jurisdictions.

|  |
| --- |
| **Additional Background—** |
|  |
| **Investigating and Prosecuting Cyber Crime** |
|  |
| To cooperate and share information with foreign agencies **investigating and prosecuting** Internet fraud, Congress enacted the Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond the Borders (U.S. Safe Web) Act of 2006. Among other things, the act also provides Internet service providers with immunity from liability (a “safe harbor”) for supplying information to the Federal Trade Commission concerning unfair or deceptive conduct in foreign jurisdictions. Following is some of the text of the U.S. Safe Web Act. |
|  |
| **15 U.S.C. Section 57c-1** |
|  |
| **Staff exchanges** |
|  |
| **(a) In general** |
|  |
| The Commission may— |
|  |
| **(1)** retain or employ officers or employees of foreign government agencies on a temporary basis as employees of the Commission pursuant to section 42 of this title or section 3101 or section 1309 of Title 5; and |
|  |
| **(2)** detail officers or employees of the Commission to work on a temporary basis for appropriate foreign government agencies. |
|  |
| **(b) Reciprocity and reimbursement** |
|  |
| The staff arrangements described in subsection (a) of this section need not be reciprocal. The Commission may accept payment or reimbursement, in cash or in kind, from a foreign government agency to which this section is applicable, or payment or reimbursement made on behalf of such agency, for expenses incurred by the Commission, its members, and employees in carrying out such arrangements. |
|  |
| **(c) Standards of conduct** |
|  |
| A person appointed under subsection (a)(1) of this section shall be subject to the provisions of law relating to ethics, conflicts of interest, corruption, and any other criminal or civil statute or regulation governing the standards of conduct for Federal employees that are applicable to the type of appointment. |
|  |
| **15 U.S.C. Section 57b-2b** |
|  |
| **Protection for voluntary provision of information** |
|  |
| **(a) In general** |
|  |
| **(1) No liability for providing certain material** |
|  |
| An entity described in paragraphs (2) or (3) of subsection (d) of this section that voluntarily provides material to the Commission that such entity reasonably believes is relevant to— |
|  |
| **(A)** a possible unfair or deceptive act or practice, as defined in section 45(a) of this title; or |
|  |
| **(B)** assets subject to recovery by the Commission, including assets located in foreign jurisdictions; |
|  |
| shall not be liable to any person under any law or regulation of the United States, or under the constitution, or any law or regulation, of any State, political subdivision of a State, territory of the United States, or the District of Columbia, for such provision of material or for any failure to provide notice of such provision of material or of intention to so provide material. |
|  |
| **(2) Limitations** |
|  |
| Nothing in this subsection shall be construed to exempt any such entity from liability— |
|  |
| **(A)** for the underlying conduct reported; or |
|  |
| **(B)** to any Federal agency for providing such material or for any failure to comply with any obligation the entity may have to notify a Federal agency prior to providing such material to the Commission. |
|  |
| **(b) Certain financial institutions** |
|  |
| An entity described in paragraph (1) of subsection (d) of this section shall, in accordance with section 5318(g)(3) of Title 31, be exempt from liability for making a voluntary disclosure to the Commission of any possible violation of law or regulation, including— |
|  |
| **(1)** a disclosure regarding assets, including assets located in foreign jurisdictions— |
|  |
| **(A)** related to possibly fraudulent or deceptive commercial practices; |
|  |
| **(B)** related to persons involved in such practices; or |
|  |
| **(C)** otherwise subject to recovery by the Commission; or |
|  |
| **(2)** a disclosure regarding suspicious chargeback rates related to possibly fraudulent or deceptive commercial practices. |
|  |
| **(c) Consumer complaints** |
|  |
| Any entity described in subsection (d) of this section that voluntarily provides consumer complaints sent to it, or information contained therein, to the Commission shall not be liable to any person under any law or regulation of the United States, or under the constitution, or any law or regulation, of any State, political subdivision of a State, territory of the United States, or the District of Columbia, for such provision of material or for any failure to provide notice of such provision of material or of intention to so provide material. This subsection shall not provide any exemption from liability for the underlying conduct. |
|  |
| **(d) Application** |
|  |
| This section applies to the following entities, whether foreign or domestic: |
|  |
| **(1)** A financial institution as defined in section 5312 of Title 31. |
|  |
| **(2)** To the extent not included in paragraph (1), a bank or thrift institution, a commercial bank or trust company, an investment company, a credit card issuer, an operator of a credit card system, and an issuer, redeemer, or cashier of travelers' checks, money orders, or similar instruments. |
|  |

|  |
| --- |
| **(3)** A courier service, a commercial mail receiving agency, an industry membership organization, a payment system provider, a consumer reporting agency, a domain name registrar or registry acting as such, and a provider of alternative dispute resolution services. |
|  |
| **(4)** An Internet service provider or provider of telephone services. |
|  |

|  |
| --- |
|  |
| Enhancing Your Lecture— |
|  |
|  Cross-Border Spam  |
|  |
| Spam is a serious problem in the United States, but enforcing antispam laws has been compli­cated by the fact that many spammers are located outside U.S. borders. After the CAN SPAM Act of 2003 prohibited false and deceptive e-mails originating in the United States, spamming from other nations increased, and the wrongdoers generally were able to escape detection and legal sanctions. |
|  |
| Before 2006, the Federal Trade Commission (FTC) lacked the authority to investigate cross-border spamming activities and to communicate with foreign nations concerning spam and other de­ceptive practices conducted via the Internet. In December 2006, however, Congress passed the U.S. Safe Web Act of 2006 (also known as the Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2006),**a** which increased the FTC’s ability to combat spam on a global level. |
|  |
| The act allows the FTC to cooperate and share information with foreign agencies in investigating and prosecuting those involved in Internet fraud and deception, including spamming, spyware, and various Internet scams. Although the FTC and foreign agencies can provide investigative assistance to one another, the act exempts foreign agencies from U.S. public disclosure laws. In other words, the activities undertaken by the foreign agency (even if requested by the FTC) will be kept secret. |
|  |
| For Critical Analysis |
|  |
| ***A provision in the U.S. Safe Web Act provides Internet service providers (ISPs) with a “safe harbor” (immunity from liability) for supplying information to the FTC concerning possible unfair or deceptive conduct in foreign jurisdictions. Is this provision fair? Why or why not?*** |
|  |
|  |
| a. Pub. L. No. 109-455, 120 Stat. 3372 (December 22, 2006), which was codified at 15 U.S.C. Sections 57b-2a, 57b-2b, 57c-1, and 57c-2, and amended other sections*.* |
|  |

# B. Domain Names

A domain name is part of an Internet address. Competition for domain names among firms with similar names and products has led to disputes. By using an identical or similar domain name, parties have attempted to profit from a competitor’s goodwill (nontangible value of a business).

1. Structure of Domain Names

Every domain name ends with a generic top-level domain (TLD), such as *.com* or *.edu*. The second-level domain is the part of the name to the left of the period of the TLD. The business or individual registering he domain name chooses this name.

2. Domain Name Distribution System

The Internet Corporation for Assigned Names and Numbers (ICANN) oversees the Internet domain name sys­tem and facilitates the resolution of domain name disputes.

## C. Cybersquatting

Disputes often involve cyber­squatting, which occurs when a person registers a domain name that is the same as, or confus­ingly similar to, another’s mark and offers to sell it to the authentic mark’s owner.

1. Anti-Cybersquatting Legislation

Problems continue because of the large number of domain-name registrars, the speed at which the names change hands, and the difficulty of tracking mass automated registrations. The text reviews the Anticybersquatting Consumer Protection Act (ACPA), which amended the Lanham Act to make cybersquatting clearly illegal when—

• The name is identical or confusingly similar to the trademark of another.

• The one registering, trafficking in, or using the domain name has a “bad faith intent” to profit from that mark.

2. Cybersquatting and the Domain Name Distribution System

Problems continue because of the speed at which the names change hands, and the difficulty of tracking mass automated registrations.

**3. Typosquatting**

This occurs when a person registers a mis­spelling of a mark that he or she does not own. To protect genuine marks, businesses register thousands of mis­spelled names.

**4. Applicability and Sanctions of the ACPA**

The ACPA applies to all domain-name registrations. Damages and profits can be awarded. Statutory damages range from $1,000 to $100,000. Difficulties include the costs of litigation and obtaining the identity of the owner of an infringing Web site. To facilitate dispute resolution, ICANN offers the Uniform Rapid Suspension (URS) system

**D. Meta Tags**

Meta tags are words in a Web site’s key-word field that determine when the site is listed in re­sponse to a search engine query. Using others’ marks as tags without permission may constitute trademark infringement.

## E. Trademark Dilution in the Online World

Dilution occurs when a mark is used, without permission, in a way that diminishes its distinc­tive quality. Proof that consumers are likely to be confused between the two marks is not required.

|  |
| --- |
| **Case Synopsis—** |
|  |
| **Case 7.1: *Hasbro, Inc. v. Internet Entertainment Group, Ltd.*** |
|  |
| Hasbro, Inc., the maker of Candyland, owns the Candyland trademark. Brian Cartmell and the Internet Entertainment Group (IEG), Ltd., used “candyland.com” as a domain name for a sexually explicit Internet site. Any person who performed an online search for “candyland” was directed to this adult Web site. Hasbro filed a trademark dilution claim in a federal court against Cartmell and IEG. |
|  |
| The court ordered the defendants to remove all content from the candyland.com site and to stop using the Candyland mark. Hasbro showed that the defendants’ use of the mark and the domain name candyland.com in connection with their site was causing irreparable injury to Hasbro. Hasbro demonstrated a likelihood of prevailing on its claims that defendants violated the applicable federal and state statutes against trademark dilution. |
|  |
| .................................................................................................................................................. |
|  |
| **Notes and Questions** |
|  |
| ***If the court had ordered both parties to change their domains, what, if any, complications would this present?*** Most likely, there would be an increase in the number of trademark disputes as the variety of domains would expand to accommodate the demands of legitimate and illegitimate businesses and individuals to change their names. Companies, individuals, and governments might find themselves embroiled in considerable amounts of litigation over the same issues noted in the case. Settlements could be expensive. |
|  |
| ***Suppose that the site using candyland.com had not been sexually explicit but had sold candy. Would the result have been the same?*** Probably. In this circumstance, Hasbro could most likely demonstrate a likelihood of prevailing on a claim that the defendant violated the applicable federal and state statutes against trademark dilution. The Hasbro is famous, the defendant would presumably be using it without permission, and that use would arguably diminish the quality of the Hasbro mark. |
|  |

## F. Licensing

Licensing (permitting the use of a file for certain purposes) is one way around many virtual property dilemmas. Licensees may be prohibited from sharing the file or using it to create similar applications. The use of the application may be limited to a specific device or for a certain time.

**II. Copyrights in Digital Information**

• Copyright law is important in cyberspace in part because the nature of the Internet means that data is “copied” before being transferred online. Loading a file or program into a computer’s random access memory (RAM) is the mak­ing of a “copy.” If it is done without authorization, it is infringement.

• The Digital Millennium Copyright Act of 1998 protects against the piracy of copyrighted materials in the online environment.

|  |
| --- |
|  |
| Enhancing Your Lecture— |
|  |
|  Legal Issues Facing |
| Bloggers and Podcasters  |
|  |
| Companies increasingly are using blogs (Web logs) and podcasts (essentially an audio blog, some­times with video clips) internally to encourage communication among employees and externally to communicate with customers. Blogs offer many advantages, not the least of which is that setting up a blog and keep it current (making “posts”) costs next to nothing because so much easy-to-use free soft­ware is available. Podcasts, even those including video, require only a little more sophistication. Nonetheless, both blogs and podcasts also carry some legal risks for the companies that sponsor them. |
|  |
| Benefits of Blogs and Podcasts |
|  |
| Internal blogs used by a company’s employees can offer a number of benefits. Blogs provide an open communications platform, potentially allowing new ways of coordinating activities among employees. For example, a team of production workers might use a blog to move a new product idea forward: the team starts a blog, one worker posts a proposal, and other team members quickly post comments in response. The blog can be an excellent way to generate new ideas. Internal blogs also al­low for team learning and encourage dialogue. When workers are spread out across the country or around the world, blogging provides a cheap means of communication that does require sophisticated project management software. |
|  |
| Many companies are also creating external blogs, which are available to clients and customers. External blogs can be used to push products, obtain feedback from customers, and shape the image that the company presents to outsider. Even some company chief executive officers (CEOs) including the CEOs of McDonald’s, Boeing, and Hewlett-Packard have started blogs. |
|  |
| Potential Legal Risks |
|  |
| Despite their many advantages, blogs and podcasts can also expose a company to a number of legal risks, including the following. |
|  |
| ***Tort Liability*** Internal blogs and podcasts can lead to claims of defamation or sexual harass­ment if an employee posts racist or sexually explicit comments. At the same time, if a company moni­tors its employees’ blogs and podcasts, it may find itself facing claims of invasion of privacy. |
|  |
| ***Security of Information*** Blogs may also be susceptible to security breaches. If an outsider ob­tains access to an internal blog, a company’s trade secrets could be lost. Outsiders could also poten­tially gain access to blogs containing financial information and other financial data. |
|  |
| ***Discovery Issues*** Litigation today frequently involves electronic dis­covery. This can extend to blog posts and comments as well as to e-mail. Thus, a company should be aware that anything posted on its blogs can be used as evidence during litigation. A company will therefore need to preserve and retain blog postings related to any dispute likely to go to trial. |
|  |
| ***Compliance Issues*** Many corporations are regulated by one or more agencies and required to comply with various statutes. Laws that require compliance may also apply to blog postings. For example, the Securities and Exchange Commission (SEC) has regulations establishing the informa­tion a company must disclose to potential investors and the public in connection with its stock. A company regulated by the SEC will find that these rules apply to blogs. The same is true for compa­nies regulated under the Sarbanes-Oxley Act. |
|  |
| ***Copyright Infringement*** Blogs can also expose a company to charges of copyright infringement. Suppose, for example, that an employee posts a long passage from a magazine article on the com­pany’s blog, either internal or external, without the author’s permission. Similarly, photos taken from other blogs or Web sites cannot be posted without prior permission. Note, also, that copyright in­fringement can occur even if the blog was created without any pecuniary motivation. Typically, though, a blogger can claim “fair use” if she or he posts a passage from someone else’s work with an electronic link to the complete version |
|  |
| External blogs carry most of the same risks as internal blogs and others as well. Not only can ex­ternal blogs lead to charges of invasion of privacy, defamation, or copyright infringement related to what the company and its employees post, but they can also expose the company to liability for what visitors post. If a company’s blog allows visitors to post comments and a visitor makes a defamatory statement, the company that created the blog could be held liable for publishing it. Thus, any com­pany considering establishing blogs and podcasts, whether internal or external, should be aware of the risks and take steps to guard against them. |
|  |
| For Critical Analysis |
|  |
| ***Do individuals who create blogs face the same risks as companies that use blogs? Explain.*** |
|  |
|  |
| a. 111 F.Supp.2d 294 (S.D.N.Y. 2000). |
| b. *Universal City Studios, Inc. v. Corley,*273 F.3d 429 (2d Cir. 2001). |
| c. *DVD Copy Control Association v. Bunner,*113 Cal.Rptr.2d 338 (2001). Note that in 2002, the California Supreme Court agreed to review this case. |
|  |

|  |
| --- |
| **Additional Background—** |
|  |
| Digital Millennium Copyright Act |
|  |
| The **Digital Millennium Copyright Act** (DMCA) of 1998 imposes penalties on anyone who circumvents encryption software or other anti-piracy protection. It also prohibits the manufacture, import, sale, or distribution of devices or services for circumvention. |
|  |
| Exceptions include the “fair use” of circumvention methods for educational and other noncommercial purposes. Internet service providers (ISPs) are also exempt from sanctions for their subscribers’ violations *unless* the ISP is aware of the violation. |
|  |
| The following is an excerpt from the DMCA. |
|  |
| Sec. 1201. Circumvention of copyright protection systems |
|  |
| **(a) VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL MEASURES—** |
|  |
| (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter. |
|  |
| (B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copy­righted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make non­infringing uses of that particular class of works under this title, as determined under subparagraph (C). |
|  |
| (C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year pe­riod, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding on the record for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make nonin­fringing uses under this title of a particular class of copyrighted works. In conducting such rulemak­ing, the Librarian shall examine— |
|  |
| (i) the availability for use of copyrighted works; |
|  |
| (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; |
|  |
| (iii) the impact that the prohibition on the circumvention of technological measures applied to copy­righted works has on criticism, comment, news reporting, teaching, scholarship, or research; |
|  |
| (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and |
|  |
| (v) such other factors as the Librarian considers appropriate. |
|  |
| (D) The Librarian shall publish any class of copyrighted works for which the Librarian has deter­mined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the pro­hibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period. |
|  |
| (E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph. |
|  |
| (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that— |
|  |
| (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; |
|  |
| (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or |
|  |
| (C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title. |
|  |
| (3) As used in this subsection— |
|  |
| (A) to `circumvent a technological measure’ means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and |
|  |
| (B) a technological measure `effectively controls access to a work’ if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work. |
|  |
| **(b) ADDITIONAL VIOLATIONS—** |
|  |

|  |
| --- |
| (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any tech­nology, product, service, device, component, or part thereof, that— |
|  |
| (A) is primarily designed or produced for the purpose of circumventing protection afforded by a tech­nological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; |
|  |
| (B) has only limited commercially significant purpose or use other than to circumvent protection af­forded by a technological measure that effectively protects a right of a copyright owner under this ti­tle in a work or a portion thereof; or |
|  |
| (C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof. |
|  |
| (2) As used in this subsection— |
|  |
| (A) to `circumvent protection afforded by a technological measure’ means avoiding, bypassing, remov­ing, deactivating, or otherwise impairing a technological measure; and |
|  |
| (B) a technological measure `effectively protects a right of a copyright owner under this title’ if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title. |
|  |
| **(c) OTHER RIGHTS, ETC., NOT AFFECTED—** |
|  |
| (1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringe­ment, including fair use, under this title. |
|  |
| (2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof. |
|  |
| (3) Nothing in this section shall require that the design of, or design and selection of parts and com­ponents for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1). |
|  |
| (4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products. |
|  |
| **(d) EXEMPTION FOR NONPROFIT LIBRARIES, ARCHIVES, AND EDUCATIONAL INSTITUTIONS—** |
|  |
| (1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph— |
|  |
| (A) may not be retained longer than necessary to make such good faith determination; and |
|  |
| (B) may not be used for any other purpose. |
|  |
| (2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form. |
|  |
| (3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1)— |
|  |
| (A) shall, for the first offense, be subject to the civil remedies under section 1203; and |
|  |
| (B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1). |
|  |

**A. Copyright Infringement**

• Digital sampling a copyrighted sound recording of any length can constitute copyright infringement. Liability can sometimes be avoided under the defense of fair use.

• Piracy of copyrighted materials includes the exchange of unauthorized copies for no profit.

|  |
| --- |
|  |
| Enhancing Your Lecture— |
|  |
|  Copyright Law versus Free Speech  |
|  |
| Since the ratification of the First Amendment to the U.S. Constitution in 1791, Congress has been prohibited from making any law “abridging the freedom of speech.” Clearly, at that time the framers did not anticipate radio, television, the movies, computers, computer programs, or the Internet. As radio, television, and the movies became important at the beginning and middle of the twentieth cen­tury, they gave rise to free speech issues. As the Internet moves into virtually everyone’s home and place of work in the twenty-first century, First Amendment issues have arisen and will continue to arise. |
|  |
| A major contemporary legal debate today concerns free speech rights in the context of intellectual property in digital form that is encrypted to prevent its unauthorized copying and use. More specifi­cally, the courts are now addressing the tension between movie studios, which are encrypting their DVDs, and “hackers” who have posted code-cracking programs on the Internet so that DVDs can be copied numerous times. |
|  |
| Applying the Digital Millennium Copyright Act of 1998 |
|  |
| Almost as soon as encryption technology was used to safeguard the contents of DVDs, the code was cracked by a group of hackers, including nineteen-year-old Norwegian John Johansen. His de­cryption program, called DeCCS, was quickly made available at various sites on the Internet includ­ing 2600.com, owned by Ed Corly. Almost immediately after DeCCS was posted, a group of movie companies, including Disney and Twentieth Century-Fox, filed suit. |
|  |
| In what was seen as a victory for the motion picture industry, a federal district court ruled, in *Universal City Studios, Inc. v. Reimerdes,***a** that DeCCS violated the Digital Millennium Copyright Act (DMCA) of 1998. As noted elsewhere, among other things the DMCA prohibits the circumvention (by decryption programs, for example) of encryption systems that are embedded in intellectual property to protect the property from piracy, or unauthorized use. The court noted that since the posting of DeCCS, along with a separate video-compression program known as DivX, the pirating of movies had become increasingly common on the Internet. |
|  |
| The defendants argued that software programs designed to break encryption schemes were a form of constitutionally protected speech. The court, however, rejected the free speech argument. “Computer code is not purely expressive any more than assassination of a political figure is purely a political statement . . . . The Constitution, after all, is a framework for building a just and democratic society. It is not a suicide pact,” stated the court. A federal appellate court affirmed the trial court’s decision.**b** |
|  |
| A Different Approach |
|  |
| In November 2001, a California appellate court reviewed a case brought by a trade association of movie industry businesses against Internet Web site operators who made DeCCS programs available from their Web sites. The trade association asked the court to enjoin the defendants from copying, distributing, publishing, or otherwise marketing the DeCCS computer program because, by doing so, the defendants were, by necessity, disclosing or using the trade secrets contained in the encryption programs. |
|  |
| The California appellate court weighed in on the side of free speech and refused to grant the in­junction. In contrast to the *Universal City Studios*decision, the court reasoned that the DeCCS pro­gram was a form of “pure speech.” Furthermore, stated the court, the “scope of protection of trade secrets does not override the protection offered by the First Amendment. The California legislature is free to enact laws to protect trade secrets, but these provisions must bow to the protections offered by the First Amendment.” The court labeled any attempt at blocking the future use of computer pro­grams “an impermissible prior restraint” on Web site operators’ First Amendment rights.**c** |
|  |
| The Debate Continues |
|  |
| If you buy a book, you can read it, throw it away, give it to someone else, or sell it to a used book­store. Once you have bought it, you can legally do just about anything with it except make copies for resale. There is no way that the owner of the intellectual property contained in that book can insert an encryption system to prevent you from letting someone else read it. In contrast, any form of digit­ized intellectual property can contain an encryption system. |
|  |
| In principle, the 1998 DMCA protects all such encryption systems from being circumvented by “code cracking.” Understandably, the movie industry is urging the courts to interpret the DMCA’s provisions against circumvention narrowly. Yet some argue that several passages in the act would seem to allow for a broader interpretation—one that would allow constitutional challenges to succeed. Ultimately, the controversy may have to be decided by the United States Supreme Court. |
|  |
| Where Do You Stand? |
|  |
| At issue in the twenty-first century is the trade-off between the necessity of writers, musicians, artists, and movie studios to profit from their work and the free flow of ideas for the public’s benefit. Movie (and music) industry participants claim that encryption programs are necessary to prevent piracy. Others, however, including the defendants in cases such as those discussed above, argue that the law should at least allow purchasers of movies, music, and books in digital form to make lim­ited copies for fair use. ***Which side of this debate do you support? Is it possible to strike an appropriate balance between the rights of both groups on this issue?*** |
|  |
|  |
| a. 111 F.Supp.2d 294 (S.D.N.Y. 2000). |
| b. *Universal City Studios, Inc. v. Corley,*273 F.3d 429 (2d Cir. 2001). |
| c. *DVD Copy Control Association v. Bunner,*113 Cal.Rptr.2d 338 (2001). Note that in 2002, the California Supreme Court agreed to review this case. |
|  |

### B. MP3 and File-Sharing Technology

**1. Methods of File Sharing**

• File sharing over the Internet can be done through peer-to-peer (P2P) networking.

• Cloud computing can deliver a single application through a browser to multiple users, or it may be a utility program to pool resources and provide data storage and servers that can be accessed on demand.

**2. Sharing Stored Music Files**

• MP3 file compression and music file sharing over the Internet through peer-to-peer (P2P) networking is generally illegal—a violation of copyright law.

• Companies that distribute file-sharing software intending it to be used to violate copyright laws can be liable for users’ copyright infringement.

**3. DVDs and File-Sharing**

File-sharing (and pirated DVDs) creates problems for the motion picture industry. Many sites offer software that facilitates the illegal copying of movies.

**III. Social Media**

Social media is the means by which people create, share, and exchange ideas and comments via the Internet.

**A. Legal Issues**

**1. Impact on Litigation**

Social media posts are routinely part of discovery in litigation. Tweets and other social media posts can also be used to reduce damages awards.

**2. Impact on Settlement Agreements**

Social media posts can be used to invalidate settlement agreements that require confidentiality.

**3. Criminal Investigations**

Social media can be used to detect and prosecute criminals.

**4. Administrative Agencies**

Federal regulators can use social media posts in their investigations. Administrative law judges can base a decision on the content of social media posts.

**5. Employers’ Social Media Policies**

Courts and employment agencies usually uphold an employer’s right to terminate a person based on his or her violation of an employer’s social media policy.

**B. The Electronic Communications Privacy Act**

Electronic monitoring may violate the Electronic Communications Privacy Act (ECPA) of 1986, which prohibits the intentional interception of any wire or electronic communication or the intentional disclosure or use of the informa­tion obtained by the interception.

**1. Exclusions**

• The “business-extension exception” permits employers to monitor employees’ electronic communications in the ordinary course of business on devices that the employer provided (but not to monitor employees’ personal communications).

• An employer can also avoid liability under the act if the employees consent to having their communications monitored.

**2. Stored Communications**

***•*** The Stored Communications Act prohibits intentional, unauthorized access to stored electronic communications.

• The act also prevents “providers” of communication services (such as social media networks) from revealing private communications to certain entities and individuals.

|  |
| --- |
|  |
| Enhancing Your Lecture— |
|  |
|  How to Develop an Internet Policy  |
|  |
| Employers that make electronic communications systems (such as access to the Internet and e-mail) available to their employees face some obvious risks. One risk is that e-mail could be used to harass other employees. Another risk is that employees could subject the employer to liability by re­producing, without authorization, copyright-protected materials on the Internet. Still another risk is that confidential information contained in e-mail messages transmitted via the Internet could be in­tercepted by an outside party. Finally, an employer that monitors employees’ Internet use in an at­tempt to avoid these risks faces yet another risk: the risk of being held liable for violating the em­ployees’ privacy rights. If you are an employer and find it prudent to monitor employees’ Internet use, you should take certain precautions. |
|  |
| Remember, a small company can be bankrupted by just one successful lawsuit against it. Even if your company wins the suit, the legal fees incurred to defend against the claim could be devastating for your profits. |
|  |
| Inform Your Employees of the Monitoring and Obtain Their Consent |
|  |
| First of all, you should notify your employees that you will be monitoring their Internet communi­cations, including their e-mail. Second, you should ask your employees to consent, in writing, to such actions. Generally, if employees consent to employer monitoring, they cannot claim that their privacy rights have been invaded by such practices. You will find it eas­ier to obtain employees’ consent to monitoring if you explain why it is necessary or desirable and let them know what methods will be used to monitor Internet communications. As a rule, when employ­ees are told the reasons for monitoring and clearly understand their rights and duties with respect to the company’s communications system, they are less offended by the surveillance. |
|  |
| Spell Out Permissible and Impermissible Internet Uses |
|  |
| Employees should be told which uses of the firm’s communications system are permissible and which uses are prohibited. To clarify Internet policy standards, develop a comprehensive policy set­ting forth your standards of Internet use and illustrate through specific examples what kinds of communications activities will constitute impermissible uses. It is also important to let employees know what will happen if they violate the policy. The policy might state, for example, that any em­ployee who violates the policy will be subject to disciplinary actions, including termination. |
|  |
| Checklist for the Employer |
|  |
| **1.** Inform employees that their Internet communications will be monitored, why monitoring is neces­sary or desirable, and how it will be conducted. |
|  |
| **2.** Obtain employees’ written consent to having their electronic communications monitored. |
|  |
| **3.** Develop a comprehensive policy statement explaining how Internet communications should and should not be used and indicating the consequences of misusing the firm’s communications system. |
|  |

**C. Protection of Social Media Passwords**

About half of the states protect individuals from having to disclose their social media passwords to employers or schools, but the laws differ. The federal government has also considered legislation.

**D. Company Social Media Networks**

Company intranets are intended for messages about deals that might be closed, new products, the details of customer orders, and other business, not the exchange of social comments.

**•** Companies can better protect their corporate secrets on internal networks by controlling employee access and maintaining secure servers.

**•** Intranets’ benefits include a reduction in the amount of e-mail and real-time information on business issues (how to sell new products, how to deal with difficult customers, and competitive information about others’ products and services).

**IV. Online Defamation**

Cyber torts are torts that arise from online conduct.

**A. Identifying the Author**

Obtaining the identity of a person who posts a defamatory remark can be accomplished through a court order.

|  |
| --- |
|  |
| **Case Synopsis—** |
|  |
| **Case 7.2: *Yelp, Inc. v. Hadeed Carpet Cleaning, Inc.*** |
|  |
| Seven users of Yelp, a social-networking consumer review Web site, posted negative reviews of Hadeed Carpet Cleaning Inc. of Alexandria, Virginia. Hadeed brought an action in a Virginia state court against the users, claiming defamation. (Hadeed alleged that the reviewers were not actual customers and thus their comments were defamatory because they falsely stated that Hadeed had provided shoddy service to each reviewer.) When Yelp failed to comply with a subpoena seeking documents revealing the users’ identities, the court held the site in contempt. Yelp appealed. |
|  |
| A state intermediate appellate court affirmed. “Without the identity of the \*  \*  \* defendants, Hadeed cannot move forward with its defamation lawsuit. There is no other option. The identity of the \*  \*  \* defendants is not only important, it is necessary.” |
|  |
| .................................................................................................................................................. |
|  |
| **Notes and Questions** |
|  |
| ***Do the Yelp posts qualify as commercial speech? If so, how does that affect the Doe defendants’ constitutional right to anonymity?*** The freedom of speech—and the freedom to speak anonymously—is not absolute.The courts have long recognized a distinction in the level of protection that the First Amendment accords to literary, religious, or political speech as compared to that accorded to commercial speech. When speech constitutes an expression related solely to the economic interests of the speaker and its audience, any First Amendment right to speak anonymously enjoys a limited measure of protection. In those cases, the First Amendment right to anonymity is subject to a substantial governmental interest in disclosure so long as disclosure advances that interest and goes no further than reasonably necessary. |
|  |
| In this case, the posts on Yelp are clearly commercial speech. They relate to, and are intended to affect, Hadeed’s reputation and its business. Thus, the posts are entitled to less protection than some other expressions. Revealing the posters’ identities advances a substantial governmental interest in their disclosure. |
|  |
| ***Should a party be required to exhaust all other means to discover the identity of an anonymous poster before an ISP can be ordered to reveal that information?*** Yes, a party should be required to exhaust all other means to discover the identity of an anonymous poster before an ISP can be ordered to reveal that information. Through exhausting all other means of identifying an anonymous poster, a party can clarify the reason that the identity is needed and demonstrate a real need for the ISP to provide that information. |
|  |

|  |
| --- |
|  |
| **Additional Cases Addressing this Issue—** |
|  |
| **Online Defamation—Identifying the Author** |
|  |
| Cases involving discovery requests seeking the identity of anonymous posters of allegedly defamatory statementsinclude the following. |
|  |
| • *Thomson v. Doe*, \_\_ Wash.App. \_\_, \_\_ P.3d \_\_, 2015 WL 4086923 (Div. 1 2015) (lawyer review Web site would not be compelled to comply with subpoena seeking identify of anonymous poster, who posted a negative review of attorney on site, when attorney failed to make a *prima facie* showing of defamation). |
|  |
| • *Geloo v. Doe,* 88 Va.Cir. 379, 2014 WL 8239928 (2014) (plaintiff failed to show that statements made on fairfaxunderground.com by anonymous posters are tortious and that plaintiff has legitimate, good faith basis to contend she is victim of actionable conduct, and thus plaintiff is not entitled to uncover identity of anonymous speakers). |
|  |
| • *Ghanam v. Does,* 303 Mich.App. 522, 845 N.W.2d 128 (2014) (in city official’s defamation action against unknown commenters who posted anonymous comments on Internet message board dedicated to discussion of local politics, comments accusing official of stealing road salt and vehicle tires could not be reasonably regarded as actionable assertions of fact) and thus motion to obtain identities would not be granted) |
|  |

**B. Liability of Internet Service Providers**

**1. General Rule**

Under the Communications Decency Act (CDA) of 1996, Internet service providers (ISPs) are not liable for the defamatory remarks of those who use their services.

**2. Exceptions**

Some courts have established some limits to ISPs’ CDA immunity.

**V. Privacy**

The right to privacy is guaranteed by at least one interpretation of the bill of rights and by some state constitutions.

**A. Reasonable Expectation of Privacy**

A person must have a reasonable expectation of privacy to maintain a suit for the invasion of privacy. This exists when entering personal banking or credit-card information online, but not in posts on Twitter or other social media.

|  |
| --- |
| **Case Synopsis—** |
|  |
| **Case 7.3: *Nucci v. Target Corp.*** |
|  |
| Maria Nucci filed a suit in a Florida state court against Target Corp., alleging that she suffered an injury when she slipped and fell on a “foreign substance” on the floor of a Target store. Target filed a motion to compel an inspection of Nucci’s Facebook profile, which included 1,249 photos. Nucci claimed that she had a reasonable expectation of privacy in the profile and Target's access would invade that privacy right. The court issued an order to compel discovery of certain photos, including some of the items on Nucci’s Facebook page. Nucci petitioned for relief from the order. |
|  |
| A state intermediate appellate court denied the petition. “The photographs sought were reasonably calculated to lead to the discovery of admissible evidence and Nucci's privacy interest in them was minimal.” |
|  |
| .................................................................................................................................................. |
|  |
| **Notes and Questions** |
|  |
| ***What did the defendant hope to gain by viewing the plaintiff’s posted photos?*** Presumably the defendant was looking for evidence that tended to show the plaintiff had not suffered an injury when she slipped and fell or that the injury was not as serious as she may have claimed. ***Why would someone post such photos?*** Nucci may have believed that her Facebook page was private, that Target would not pursue discovery of the photos—because, perhaps, the defendant or its insurance company would prefer to settle rather than litigate her claim—or the posting may have been thoughtless. ***Suppose that the photos show what Target hopes to discover—that the plaintiff’s claim was not supported by the facts. What are the ethics of seeking to recover for an injury that did not occur?*** |
|  |

**B. Data Collection and Cookies**

Cookies (invisible files that computers and mobile devices create to track a user’s browsing activities) provide information to marketers about an individual’s behavior and preferences. Does this violate a user’s privacy? Does selling or otherwise using the data violate privacy?

**C. Internet Companies’ Privacy Policies**

The Federal Trade Commission (FTC) investigates consumer complaints of privacy violations and has Internet companies’ consent to review their privacy practices.

**D. Protecting Consumer Privacy**

The goal of the proposed “Consumer Privacy Bull of Rights” is to ensure that consumers’ personal information is safe online.

|  |
| --- |
|  |
| **Teaching Suggestions** |
|  |
| **1.** It could be pointed out that disputes arising in the areas covered in this chapter, particularly those related to intellectual property, are among the most volatile and most extensively—and expensively—litigated disputes in the law. |
|  |
| **2.** Ask students to research online the following question: ***how does a business choose and protect a domain name?*** (1) Find out if a name is taken (there are firms that run global searches). (2) Register the name. (3) Consider: (a) the risks of not registering in countries other than the United States (***for instance, do you do business abroad? do you have foreign competitors?*** etc.); (b) the costs of registering elsewhere (about $250 per country, with as many as two hundred countries in which to register); and (c) the complica­tions of registering elsewhere (technical and regulatory subjects to deal with in each country—requirements, fees, language translations, currency conversion, etc.). (4) Hire a professional registration service to do everything. |
|  |
| 3. More than most of the other chapters in this textbook, the material in this chapter can be researched online. As of this writing, most, if not all, of the cases set out in this chapter can also be found at more than one Web site. Ask students to go online and update any of the individual cases or topics discussed in the text. Ask stu­dents, when undertaking this research, to evaluate the sources of the material that they find on the Web. *How do you know when a source is reliable?* |
|  |
| **4.** Students may be surprised to learn that their e-mail may not be private, technologically or le­gally, when it is sent or received through their workplace. Students might be asked to discuss the advantages and disadvantages of this circumstance. ***Would they rather work for an employer who monitors their communications or one who does not? Why?*** |
|  |
| *Cyberlaw Link* |
|  |
| Questions that students might be asked include the following. |
|  |
| ***• Is linking to a Web site without authorization an infringement of the site’s copyright? Is it a violation of trademark law? Would it make any difference if the URL included a person’s name or a trademark?*** |
|  |
| ***• Should the laws that govern the topics discussed in this chapter be made uniform throughout the world? Should there always be different laws for different technologies?*** |
|  |
| ***• Should a company be entitled to monitor the use of its products after they have been sold? If so, should it be a crime to resist this monitoring?*** |
|  |
| ***• What are the legal questions and complications of monitoring employees’ use of the Internet during working hours? What are some of the key points of a good policy regarding the use, and monitoring of the use, of the Internet in the workplace?*** |
|  |

**Discussion Questions**

**1. *Do Internet service providers have an ethical duty to advise their users if the in­formation that the users provide for distribution through the ISPs might violate the law? Explain.*** Yes, because such advice could remind users of the limits on information that may be dis­tributed online, just as posted speed limits remind motorists of how fast they can safely and legally drive. No, because this might have a “chilling” effect on the user’s speech—that is, on the information that the users would otherwise provide. Also, it could be considered to constitute the unauthorized practice of laws.

**2. *Should the courts continue to regard the CDA’s grant of immunity to Internet service providers as vigorously as in the past? Why or why not?*** One of Congress's goals in enacting the CDA was to encourage “the unfet­tered and unregulated development of free speech on the Internet.” So long as this goal is considered important, the CDA’s grant of immunity to Internet service providers should arguably be considered “robust.” If this speech is perceived as fairly well developed, or to have become the online equivalent of a shout of “Fire!” in a crowded theater, however, it might be argued that the immunity has served its purpose and could be restrained.

**3. *Why are Internet service providers (ISPs) exempt from liability, under some statutes, for the actions of their customers?*** Sometimes it is viewed as unfair to impose liability on an ISP for the actions of its customers, who may number in the hundreds of thousands, or more. It also sometimes said that imposing such liability would inhibit the development of the Web and the Internet. An analogy might be the imposition of liability on a bookseller for the statements of every author in every book that the seller sold. To so restrict ISPs (or booksellers) would limit access to their products and services to very few customers.

**4.** ***How might a file-sharing system, or a similar service, be put to commercially significant but nonfringing uses?*** One possibility is that the service could pay copyright owners before allowing the transmission of their material via the Internet and charge its Web site’s users to down­load that material. The same might be done with other types of intellectual property—movies, books, etc.

**5. *As social media becomes ever more pervasive, what can be expected to occur with respect to trademark disputes?***There will be an increase in the number of trademark disputes as the Internet expands worldwide and becomes part of more and more people’s lives. Even in China, a country not known for its protection of intellectual property—particularly foreigners’ intellectual property—Apple Inc. had to pay $60 million to settle a trademark dispute concerning the iPad.

**6.** ***Why is copyright law important in cyberspace?*** The public interest in copyright law is the interest in upholding copyrighted protection. If there were no protection for mu­sic and other works of intellectual and creative processes, or if the copyright laws were not enforced, there would be less incentive to produce, package, and market such works. Our lives would be less rich in their absence. Copyright is important in cyberspace in part because the nature of the Internet means that data is “copied” before being transferred online. Loading a file or program into a computer’s random access memory (RAM) is the mak­ing of a “copy.” If it is done without authorization, it is infringement. Criminal piracy includes persons who exchange unauthorized copies of copyrighted works, even for no profit.

**7.**  ***Could the winner of an Academy Award, or a Heisman Trophy, or any other award with a familiar title, use that trademark as a meta tag for a Web site?*** Probably. The outcome in any case would depend on the factors applied in the *Welles* case. If the circumstances were similar, however, it is likely that the result would be the same. ***Could someone who has not won such an award use the trademark as a tag?*** This would also depend on the factors mentioned in the Welles case. If the use of the mark on the Web site were editorial—an article discussing contenders for Academy Awards, for example—it would not seem inappropriate to permit the use of the trademark as a tag.

**8.**  ***Why is it important to protect trademarks from trademark dilution and cybersquatting?*** As stated in Article I, Section 8, of the Constitution, Congress is authorized “[t]o promote the Progress of Science and useful Arts, by se­curing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.” Laws protecting trademarks, as well patents and copyrights, are designed to pro­tect and reward inventive and artistic creativity.

**9.** ***Are there creative works that can be shared or otherwise used by anyone without permission and without the payment of royalties?*** Yes. Works in the public domain can be used by anyone without permission and without the payment of royalties. ***What is “the public domain”?*** This term means “not in copyright.” ***Why is this significant to musicians, conductors, publishers, and others?***

**10. *Considering the anonymous nature of the Internet, has defamation become an outdated legal concept?*** Each day in blogs around the world, statements are posted that constitute libel. The cost of tracking down the person who made the libelous statement is too high to justify bringing a suit against that person, however.  And even if a suit is filed and won, other Internet users will post additional libelous statements. Of course, simply ignoring libelous statements posted on the Web will only encourage such statements.  If individuals and companies that have been libeled stand up against libelous bloggers, then others will think twice about posting libelous statements.  Defamation law should be enforced as always.

**Activity and Research Assignments**

**1.** News reports of local, national, and international developments involving the topics in this chapter occur daily and can be used in covering and expanding on this material. Events that are cur­rently widely publicized involve Internet law, social media, and privacy issues. Students can spot these and discuss them in class.

**2.** In discussing trademark dilution, ask students to bring to class examples of marks and infringing marks. Discuss as a large group whether the examples are properly identified.

**Explanations of Selected Footnotes in the Text**

**Footnote 9:** Bridgeport Music, Inc., and Westbound Records, Inc., own the copyright to “Get Off Your Ass and Jam,” which opens with a three-note solo guitar riff that lasts four seconds. The rap song “100 Miles and Runnin” contains a two-second sample from the guitar solo, at a lower pitch, looped and extended to sixteen beats, in five places in the song, with each looped segment lasting about seven seconds. “100 Miles” was included in the sound track of the movie *I Got the Hook Up*, which was distributed by No Limit Films. Bridgeport, Westbound, and others filed a suit in a federal district court against No Limit and others, alleging copyright infringement. The court issued a summary judgment in the defendants’ favor. Westbound appealed. In ***Bridgeport Music, Inc. v. Dimension Films,*** the U.S. Court of Appeals for the Sixth Circuit reversed. Digitally sampling a copyrighted sound recording of any length is copyright infringement. “[A] sound recording owner has the exclusive right to ‘sample’ his own recording.” In other words, “the world at large is free to imitate or simulate the creative work fixed in the recording so long as an actual copy of the sound recording itself is not made. .  .  . Get a license or do not sample,” because “even when a small part of a sound recording is sampled, the part taken is something of value. “

***Suppose that instead of a sound recording, this case had involved three seconds of a copyrighted movie, which the defendants pirated off the Internet and incorporated as back­ground in a music video production. Would this court’s holding be different?*** The result probably would have been the same, based on the same reasoning. The owner of the copyright in a film has the exclusive right to its use. Licensing is always possible.

***Who is most likely to perceive the holding in this case—which arguably sets out a new rule—to “stifle creativity”?*** The court stated, “Since digital sampling has become so commonplace and rap music has become such a significant part of the record industry, it is not surprising that there are probably a hundred articles dealing with sampling and its ramifications. It is also not sur­prising that the viewpoint expressed in a number of these articles appears driven by whose ox is be­ing gored. As is so often the case, where one stands depends on where one sits. For example, the sound recording copyright holders favor this interpretation as do the studio musicians and their la­bor organization. On the other hand, many of the hip hop artists may view this rule as stifling crea­tivity. The record companies and performing artists are not all of one mind, however, since in many instances, today’s sampler is tomorrow’s sample. The incidence of ‘live and let live’ has been rela­tively high, which explains why so many instances of sampling go unprotested and why so many sampling controversies have been settled.”

***How can artists sample others’ works and avoid liability for infringement?*** The court ex­plained, “[M]any artists and record companies have sought licenses as a matter of course. Since there is no record of those instances of sampling that either go unnoticed or are ignored, one cannot come up with precise figures, but it is clear that a significant number of persons and companies have elected to go the licensing route. Also there is a large body of pre-1971 sound recordings that is not protected and is up for grabs as far as sampling is concerned. Additionally, just as many artists and companies choose to sample and take their chances, it is likely that will continue to be the case.”

***Suppose that rather than taking a few notes from another’s musical composition,* No Limit *had played the exact same notes in the studio when recording. In other words, the band did not “sample” the copyrighted work of another. How would this change the outcome of the case? Could Bridgeport and Westbound still prove copyright infringement?*** The result might have been the same, based on the same reasoning. The owner of the copyright to a song has the exclusive right to its use. Licensing is always possible. No Limit might have avoided liability if it could have proved that it had never heard the copyrighted piece.

**Footnote 21:** Roommates.com, LLC, operates an online roommate matching Web site and e-mail newsletter. Users disclose information about themselves and their roommate preferences based on age, gender, and other characteristics, and on whether children will live in the household. The Fair Housing Councils of San Fernando Valley and San Diego, California, filed a suit in a federal district court against Roommates.com, claiming that a violation of the Fair Housing Act (FHA). The court held that the Communications Decency Act (CDA) barred this claim and dismissed it. The Councils appealed. In ***Fair Housing Council of San Fernando Valley v. Roommates.com, LLC,*** the U.S. Court of Appeals for the Ninth Circuit concluded that the CDA does not immunize Roommates.com for all of the content on its Web site and in its e-mail newsletters. Roommates.com is “the ‘information content provider’ as to the questions and can claim no immunity for posting them on its Web site, or for forcing subscribers to answer them as a condition of using its services.” The appellate court re­versed the lower court’s summary judgment, and remanded the case for a determination of whether Roommates.com’s acts violated the FHA.

Members of Roommates.com’s service can add “Additional Comments” to their Web-generated profiles through an open-ended essay prompt. ***Does the CDA exempt Roommate from liability for pub­lishing the content its members provide in the “Additional Comments” portion of their pro­files?*** In an earlier opinion, the same court concluded that “Roommate's involvement is insufficient to make it a content provider of these comments. Roommate's open-ended question suggests no particular information that is to be provided by members; Roommate certainly does not prompt, encourage or solicit any of the inflam­matory information provided by some of its members. Nor does Roommate use the information in the ‘Additional Comments’ section to limit or channel access to listings. Roommate is therefore not re­sponsible, in whole or in part, for the creation or development of its users' answers to the open-ended ‘Additional Comments’ form, and is immune from liability for publishing these responses.”.