*Chapter 5*

**Internet Law,**

**Social Media, and Privacy**

**Answers to Learning Objectives/**

**Learning Objectives Check Questions**

**at the Beginning and the End of the Chapter**

**Note that your students can find the answers to the even-numbered *Learning Objectives Check* questions in Appendix E at the end of the text. We repeat these answers here as a convenience to you.**

**1A. *What is cybersquatting, and when is it illegal?*** Cybersquattingoccurs when a person registers a domain name that is the same as, or confusingly similar to, the trademark of another and then offers to sell the domain name back to the trademark owner.

Cybersquatting is illegal under the Anticybersquatting Consumer Protection Act when (1) the name is identical or confusingly similar to the trademark of another and (2) the one registering, trafficking in, or using the domain name has a “bad faith intent” to profit from that trademark.

**2A. *What steps have been taken to protect intellectual property rights in the digital age?*** The steps that have been taken to protect intellectual property in to­day’s digital age include the application of traditional and existing law in the cy­ber context. For example, the passage of such federal laws as the Digital Millennium Copy­right Act, and the drafting of such state laws as the Uniform Electronic Transactions Act (UETA) are major steps in protecting intellectual property rights. Additionally, the signing of such treaties as the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement and the World Intellectual Property Organization (WIPO) Copyright Treaty add protection on a global level.

**3A. *When does the law protect a person's electronic communications from being intercepted or accessed?*** The Electronic Communications Privacy Act (ECPA) amended federal wiretapping law to cover electronic forms of communications. The ECPA prohibits the intentional interception of any wire, oral, or electronic communication.

Part of the ECPA is known as the Stored Communications Act (SCA). The SCA prohibits intentional and unauthorized access to *stored* electronic communications. A person can violate the SCA by intentionally accessing a stored electronic communication.

Excluded from the ECPA’s coverage are communications through devices—such as a cell phone, laptop, or tablet—that an employer provides for its employee to use “in the ordinary course of its business.” An employer can also avoid liability under the act if the employees consent to having their electronic communications monitored by the employer.

**4A. *What law governs whether Internet service providers are liable for online defamatory statements made by users?*** The Communications Decency Act (CDA) sets out the liability of Internet service providers (ISPs) for online defamatory statements made by users.

Under the CDA, “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” Thus, an ISP is usually not liable for the publication of a user’s defamatory statement. This is a broad shield, and some courts have established some limits. For example, an ISP that prompts its users to make such statements would likely not be permitted to avoid liability for the statements.

**5A. *How do online retailers track their users' Web browsing activities?*** Whenever consumers purchase items from an online retailer, the retailer uses cookies to collect information about the consumer. Cookies are invisible files that computers, smartphones, and other mobile devices create to track a user’s Web browsing activities. Cookies provide detailed information to marketers about an individual’s behavior and preferences, which is then used to personalize online services.

## Answers to Critical Thinking Questions

**at the Ends of the Features**

**Adapting the Law to the Online Environment—Critical Thinking**

***Sony revealed that the script for a new James Bond movie had been hacked and leaked. Could a news publication legally print or post online that entire script? Why or why not?*** Any organization that would publish an entire script would be guilty of copyright infringement. So, the script could, of course, be posted on online, but whoever was responsible for such posting would be in violation of copyright law and could be vigorously pursued in court.

**Beyond Our Borders—Critical Thinking**

***How could the “right to be forgotten” affect free speech?*** Google’s forced filtering of search results might affect freedom of communication and a people’s right to educate themselves about other people. The “right to be forgotten” ruling sidesteps existing legal procedures. It forces Google to be responsible for the content that appears in its result, making it to some extent an editor. If search engines are forced to remove links to legitimate content that is already in the public domain, but not the content itself, this could lead to online censorship. Parker Higgins, an Electronic Frontier Foundation activist stated that “Limiting what sorts of things search engines can link to . . . is a specialized area of speech, but its real speech. And it affects what kinds of news people can discuss. It puts a chilling effect on journalist’s reporting and to what they can link.”

**Answers to Critical Thinking Questions**

**at the Ends of the Cases**

**Case 5.2—Critical Thinking—Ethical Consideration**

***Why would someone post a negative review of a business that he or she had never patronized? Discuss the ethics of this practice.*** Someone might post a negative review of a business he or she had never patronized for a variety of commercial or personal reasons. The poster might be an unscrupulous competitor or a vindictive friend, relative, or acquaintance of the owner or an employee. Of course, in any circumstance, as long as the poster is attesting to events that did not actually occur, the post would be a lie and thus unethical.

**Case 5.3—What If the Facts Were Different?**

***Suppose that Target had asked for a much broader range of Facebook material that concerned not just Nucci’s physical and mental condition at the time of her alleged injury but her personal relationships with her family, romantic partners, and other significant others. Would the result have been the same? Discuss.*** It is not likely that the result in this case would have been the same if Target had asked for a much broader range of Facebook material that concerned not just Nucci’s physical and mental condition at the time of her alleged injury but her personal relationships with her family, boyfriends, husbands, and other significant others. This request would have been overbroad, seeking personal information that was not relevant to the issues in the case.The discovery actually ordered in the *Nucci* case was narrower in scope and calculated to lead to evidence admissible in court.

**Answers to Questions in the Reviewing Feature**

**at the End of the Chapter**

**1A.** ***Downloading***

Technology has vastly increased the potential for copyright infringement. Generally, whenever a party downloads music into a computer’s random access memory, or RAM, without authorization, a copyright is infringed. Thus, when file-sharing is used to download others’ stored music files, copyright issues arise. Recording artists and their labels stand to lose large amounts of royalties and revenues if relatively few digital downloads or CDs are purchased and then made available on distributed networks.

**2A.** ***Sampling***

At least one federal court has held that sampling a copyrighted sound recording of any length constitutes copyright infringement. Some other federal courts have not found that digital sampling is always illegal. Some courts have allowed the defense of fair use, while others have not.

**3A.** ***Posting***

Piracy of copyrighted materials online can occur even if posting the materials is “altruistic” in nature—unauthorized copies are posted simply to be shared with others. The law extends criminal liability for the piracy of copyrighted materials to persons who exchange unauthorized copies of copyrighted works without realizing a profit.

**4A.** ***Passwords***

By 2016, about half of the states had enacted legislation to protect individuals from having to disclose their social media passwords. The federal government is also considering legislation that would prohibit employers and schools from demanding passwords to social media accounts. If, at the time of the application, however, Massachusetts was not covered by any of these statutes, Boston University would not have violated any law by asking for Gibbs’s password, which he then voluntarily divulged.

**Answer to** **Debate This Question in the Reviewing Feature**

**at the End of the Chapter**

***Internet service providers should be subject to the same defamation laws as newspapers, magazines, and television and radio stations.*** Those who support this position argue that it is not fair to those who are defamed by others on the Internet to not have recourse against the ISP. After all, there should be no difference between traditional media outlets and the Internet. Those who are against applying similar defamation law to all media argue that ISPs cannot become censors. They point out the technological inability of ISPs to monitor all of the statements that go through their servers.

**Answers to Issue Spotters**

**at the End of the Chapter**

**1A.** ***Karl self-publishes a cookbook titled* Hole Foods*, in which he sets out recipes for donuts, Bundt cakes, tortellini, and other foods with holes. To publicize the book, Karl designs the Web site* holefoods.com*. Karl appropriates the key words of other cooking and cookbook sites with more frequent hits so that* holefoods.com *will appear in the same search engine results as the more popular sites. Has Karl done anything wrong? Explain.*** Karl may have committed trademark infringement. Search engines compile their results by looking through Web sites’ key-word fields. Key words, or meta tags, increase the likelihood that a site will be included in search engine results, even if the words have no connection to the site.

A site that appropriates the key words of other sites with more frequent hits will appear in the same search engine results as the more popular sites. But using another’s trademark as a key word without the owner’s permission normally constitutes trademark infringement. Of course, some uses of another’s trademark as a meta tag may be permissible if the use is reasonably necessary and does not suggest that the owner authorized or sponsored the use.

**2A.** ***Eagle Corporation began marketing software in 2001 under the mark “Eagle.” In 2013, Eagle.com, Inc., a differ­ent company selling different products, begins to use* eagle *as part of its URL and registers it as a domain name. Can Eagle Corporation stop this use of* eagle*? If so, what must the company show?*** Yes. This may be an instance of trademark dilution. Dilution occurs when a trademark is used, without permission, in a way that diminishes the distinctive quality of the mark. Dilution does not require proof that consumers are likely to be confused by the use of the unauthorized mark. The products involved do not have to be similar. Dilution does require, however, that a mark be famous when the dilution occurs.

**Answers to Business Scenarios and Case Problems**

**at the End of the Chapter**

**Business Scenarios and Case Problems**

**5–1A. *Internet service providers***

No, CyberConnect is not regarded as a publisher and therefore is not liable for the content of Market Reach’s ad. The Communications Decency Act (CDA) states that “no provider \*  \*  \* of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” In other words, under the CDA, CyberConnect and other ISPs are treated differently from most publishers in print and other media and are not liable for the content of published statements, such as the Market Reach’s ad in this problem, that come from a third party.

**5–2A. *Privacy***

Initially, SeeYou’s best option in this situation might be to give members the opportunity to prevent the broadcast of any private information by requiring their consent. Otherwise, the members could legitimately complain that the new program was causing publication of private information without their permission. Or SeeYou might allow members to affirmatively opt out of the program altogether. Of course, SeeYou might also discontinue the program. And if any of the members decide to file a suit against SeeYou for violations of federal or state privacy statutes, the firm might offer to settle to avoid further complaints and negative publicity.

**5–3A. *Copyrights in digital information***

Yes, Thomas-Rasset is liable for copyright infringement. File-sharing is accomplished through peer-to-peer (P2P) networking. When file-sharing is used to download others’ stored music files, copyright issues arise. The issue of infringement in file-sharing has been a subject of debate since the cases against Napster, Inc. and Grokster, Ltd., two companies that created software used to share files in infringement of others’ copyrights. Napster operated a Web site with free software that enabled users to copy and transfer MP3 files via the Internet. Firms in the recording industry sued Napster. Ultimately, the court held Napster liable for copyright infringement.

Here, Thomas-Rasset willfully infringed Capitol’s intellectual property rights under the Copyright Act by making twenty-four songs available for distribution on an online peer-to-peer network. Her subsequent effort to conceal her actions by changing the hard drive on her computer showed a proclivity for unlawful conduct. This would support imposing an injunction on Thomas-Rasset against making songs or any recordings available for distribution to the public through a P2P or any other online media distribution system.

In the actual case on which this problem is based, Capitol filed a suit in a federal district court against Thomas-Rasset, who was found liable for copyright infringement and assessed damages of $54,000. On appeal, the U.S. Court of Appeals for the Eighth Circuit vacated the lower court's judgment, concluding that it should have assessed statutory damages of at least $222,000 and should have enjoined Thomas-Rasset from making copyrighted works available to the public. The appellate court remanded the case with directions to enter a judgment that included those remedies.

**5–4A. *Domain names***

Yes, Austin is entitled to a transfer of the domain names. At times, by using an identical or similar domain name, parties attempt to profit from the goodwill of a competitor or other successful company. For example, a party might use a similar domain name to sell pornography, offer for sale another party’s domain name, or otherwise infringe on others’ trademarks. Cybersquatting occurs when a person registers a domain name that is the same as, or confusingly similar to, the trademark of another. The Anticybersquatting Consumer Protection Act (ACPA) makes cybersquatting illegal when (1) the name is identical or confusingly similar to the trademark of another and (2) the one registering, trafficking in, or using the domain name has a “bad faith intent” to profit from that trademark. The ACPA applies to all domain name registrations of trademarks.

In this problem, the current registrant of the eight domain names is acting with a bad faith intent to profit. First, the names are identical to those previously used by Austin. Second, the registrant is not the true owner of the names—they were taken from Austin, the true owner, without permission and illegally transferred to a fraudulent registrant. Thus, the current registrant lacks any basis to claim them and does not have any trademark or other intellectual property rights in them. Third, the registrant is not using the names to display sites that use Austin’s marks in a genuine noncommercial or fair use manner. The names are being used to host malicious content—to send customers hate letters and to post customers' credit card numbers and other private information. In this way, the registrant is harming Austin’s goodwill and business reputation. Also, the contact information for the registrant is fraudulent and designed to obscure the true identity of the illegal actors.

In the actual case on which this problem is based, the court ordered the domain name registrar to transfer the names back to Austin.

**5–5A. Business Case Problem with Sample Answer—*Privacy***

No, Rolfe did not have a privacy interest in the information obtained by the subpoenas issued to Midcontinent Communications. The courts have held that the right to privacy is guaranteed by the U.S. Constitution’s Bill of Rights, and some state constitutions contain an explicit guarantee of the right. A person must have a reasonable expectation of privacy, though, to maintain a suit or to assert a successful defense for an invasion of privacy.

People clearly have a reasonable expectation of privacy when they enter their personal banking or credit card information online. They also have a reasonable expectation that online companies will follow their own privacy policies. But people do not a reasonable expectation of privacy in statements made on Twitter and other data that they publicly disseminate. In other words, there is no violation of a subscriber’s right to privacy when a third-party Internet provider receives a subpoena and discloses the subscriber’s information.

Here, Rolfe supplied his e-mail address and other personal information, including his Internet protocol address, to Midcontinent. In other words, Rolfe publicly disseminated this information. Law enforcement officers obtained this information from Midcontinent through the subpoenas issued by the South Dakota state court. Rolfe provided his information to Midcontinent—he has no legitimate expectation of privacy in that information.

In the actual case on which this problem is based, Rolfe was charged with, and convicted of, possessing, manufacturing, and distributing child pornography, as well as other crimes. As part of the proceedings, the court found that Rolfe had no expectation of privacy in the information that he made available to Midcontinent. On appeal, the South Dakota Supreme Court upheld the conviction.

**5–6A. *File-sharing***

The facts of this case indicate that the security of private information in any database accessible from the Web is weak. And this information can be easily shared with others through peer-to-peer networks, which allow users to place shared computer files in folders that are open for other users to search.

As part of the research for their article, Johnson and Tiversa searched the networks for data that could be used to commit medical or financial identity theft. On one of them, they found a document that contained the Social Security numbers, insurance information, and treatment codes for patients of LabMD, Inc. Tiversa notified LabMD of the find. LabMD appeared not to have willingly revealed this information because on learning of its exposure, the company filed a suit against Tiversa.

In the actual case on which this problem is based, the court dismissed the suit for lack of personal jurisdiction over Tiversa. On appeal, the U.S Court of Appeals for the Eleventh Circuit affirmed. LabMD asserted jurisdiction under a long-arm statute of Georgia. But Tiversa was not registered to do business in Georgia, had no employees or customers in Georgia, derived no revenue from business activities in Georgia, owned no Georgia property, and paid no Georgia taxes. Furthermore, although accessible in Georgia, Tiversa’s Web site merely advertised its services, and did not offer products or services for purchase online. Tiversa's entire contact with Georgia consisted of one phone call and nine e-mails to LabMD. This was not sufficient.

**5–7A. *Social media***

As stated in the text, law enforcement can use social media to detect and prosecute suspected criminals. But there must be an authenticated connection between the suspects and the posts. To make this connection, law enforcement officials can present the testimony or certification of authoritative representatives of the social media site or other experts. The posts can be traced from the pages on which they are displayed and the accounts of the “owners” of the pages to the posters through Internet Protocol (IP) addresses. An IP address can reveal the e-mail address, and even the mailing address, of an otherwise anonymous poster.

The custodians of Facebook, for example, can verify Facebook pages and posts because they maintain those items as business records in the course of regularly conducted business activities. From those sources, the prosecution in Hassan’s case could have tracked the IP address to discover his identity.

In the actual case on which this problem is based, on Hassan’s appeal of his conviction, the U.S. Court of Appeals for the Fourth Circuit affirmed.

**5–8A. *Social media***

Yes, a reasonable person could conclude that Wheeler’s posts were “true” threats. Law enforcement uses social media to detect and prosecute criminals. Police may also use social media to help them to locate a particular suspect or to determine his or her identity.

In this problem, Kenneth Wheeler was angry at police officers in Grand Junction, Colorado, due to a driving-under-the-influence arrest that he viewed as a set-up. While in Italy, Wheeler posted a statement to his Facebook page urging his “religious followers” to “kill cops, drown them in the blood of their children, hunt them down and kill their entire bloodlines” and provided names. Later, Wheeler added a post to “commit a massacre in the stepping stones preschool and day care, just walk in and kill everybody.” In determining whether a “true” threat has been made, a court asks whether those who hear or read the threat reasonably consider that an actual threat has been made. Exhortations to unspecified others to commit violence can amount to true threats, so as to support a criminal prosecution based on those threats, especially if a reasonable person might believe the individuals ordered to take violent action are subject to the will of the threatening party. Law enforcement officers might use Wheeler’s posts to detect, investigate, and prosecute any crimes. Police may also use the posts to help them to determine Wheeler’s identity and his location.

In the actual case on which this problem is based, Wheeler was convicted of transmitting a threat and sentenced to forty months' imprisonment. On appeal, the U.S. Court of Appeals for the Tenth Circuit held that a reasonable person could interpret Wheeler’s statements to be “true” threats. The court remanded the case for a new trial on other grounds.

**5-9A. A Question of Ethics—*Criminal investigations***

**1.** The government would want to “seal” the documents of an investigation to maintain secrecy. For example, the sealed documents could contain sensitive nonpublic facts, including the identity of targets and witnesses in an ongoing criminal investigation. This is most likely the purpose for the sealing of the documents in the facts of this case.

The individuals under investigation might want those documents to be “unsealed” to anticipate what information is sought, to learn what information has been found, and to prepare a defense to possible charges or to take other actions to avoid a violation of their constitutional rights. This may be the reason that the individuals in this problem filed a suit to unseal the records in the investigation of their case.Also, the public has an interest in openness and a common law right of access to judicial records, which can include the documents at issue here.

In balancing the government's interest in secrecy, individuals’ right to mount a defense, and the public's right to access court orders and proceedings, a court does not want to jeopardize the investigation. A court would consider the following factors: (1) whether any of the parties is seeking the documents or other records for an improper purpose, such as promoting a public scandal or unfairly gaining a business advantage; (2) whether the unsealing of the documents or their release would enhance the public's understanding of an important historical event; and (3) whether the public has already had access to the information contained in the documents.

In the actual case on which this problem is based, the court that approved the subpoenas refused to unseal the documents in the investigation. On appeal, the U.S. Court of Appeals for the Fourth Circuit upheld this decision. The “government's interests in maintaining the secrecy of its investigation, preventing potential subjects from being tipped off, or altering behavior to thwart the government's ongoing investigation outweighed the interests” of the Twitter subscribers.

**2.** Law enforcement uses social media to detect and prosecute criminals. Social media posts are routinely part of discovery in civil litigation because they can provide damaging information that establishes what a person knew at a particular time or the person’s intent. Like e-mail, posts on social networks can be the smoking gun that leads to liability. Similarly, in a criminal prosecution, social media posts can establish the same elements and provide evidence of criminal activities—a smoking gun that leads to guilt.

Generally, this use of social media is not an illegal invasion of individuals’ privacy. Whether it is *unethical* may be a question of personal values and perspective. Some persons may find it objectionable because it is the government engaging in this practice. Others may find it acceptable based on the motives of the investigators and those investigated in an individual case. Whatever the ethics behind a particular perspective, some version of the factors listed above will likely be applied to come to a conclusion.

**Critical Thinking and Writing Assignments**

**5-10A. Business Law Critical Thinking Group Assignment—*File-sharing***

**1.** Just because the three roommates are not profiting from their file sharing actions does not mean that they wouldn’t be subject to copyright law. A copyright violation can occur in the absences of any monetary benefit. Congress extended liability under copyright law to persons who exchange unauthorized copyrighted words without realizing a profit.

**2.** The purchaser of a CD has the right to loan or sell that CD to anyone else. If the roommates each rip the CD to their own hard drives, generally, there will be no copyright violation.