Instructor Manual

Miller, Business Law Today – Comprehensive Edition: Text and Cases 13e 2022, 9780357634783; Chapter 8: Internet Law, Social Media, and Privacy

Table of Contents

[Purpose and Perspective of the Chapter 2](#_Toc62464977)

[Cengage Supplements 2](#_Toc62464978)

[Chapter Objectives 2](#_Toc62464979)

[Key Terms 2](#_Toc62464980)

[What's New in This Chapter 3](#_Toc62464981)

[Chapter Outline 4](#_Toc62464982)

[Discussion Questions 7](#_Toc62464983)

[Additional Activities and Assignments 9](#_Toc62464984)

[Additional Resources 10](#_Toc62464985)

[Cengage Video Resource 10](#_Toc62464986)

#

# Purpose and Perspective of the Chapter

 The purpose of this chapter is for students to learn the principles that guide the amended laws and new legislation for digital technology, 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. Students will learn that being aware of the legal changes in these fields is part of doing business successfully.

# Cengage Supplements

The following product-level supplements provide additional information that may help you in preparing your course. They are available in the Instructor Resource Center.

* Transition Guide (provides information about what’s new from edition to edition)
* Test Bank (contains assessment questions and problems)
* Solution and Answer Guide (offers textbook solutions and feedback)
* PowerPoint (provides text-based lectures and presentations)
* Guide to Teaching Online (provides technological and pedagogical considerations and resources for teaching online)
* MindTap Educator Guide (describes assets in the MindTap platform with a detailed breakdown of activities by chapter with seat time)

# Chapter Objectives

The following objectives are addressed in this chapter:

1. Identify potential torts related to the use of the internet.
2. Identify when user generated content may be regulated.
3. Describe the rights and duties of internet service providers.
4. Explain when law enforcement may access a user’s social media content.
5. Explain when an employer may access an employee’s social media content.
6. Describe how unsolicited electronic communications are regulated under federal law.

[[return to top]](#_top)

# Key Terms

**Cloud computing**: the delivery to users of on-demand services from third-party servers over a network.

**Cookie**: a small file sent from a website and stored in a user’s Web browsing activities.

**Cybersquatting**: the act of registering a domain name that is the same as, or confusingly similar to, the trademark of another and then offering to sell that domain name back to the trademark owner.

**Cyber tort**: a tort committed via the Internet.

**Distributed network**: a network that can be used by persons located (distributed) around the country or the globe to share computer files.

**Domain name**: the series of letters and symbols used to identify a site operator on the Internet (an Internet address).

**Goodwill**: in the business context, the valuable reputation of a business viewed as an intangible asset.

**Internet service providers (ISP)**: a business or organization that offers users access to the Internet and related services.

**Peer-to-peer (P2P) networking**: the sharing of resources among multiple computer or other devices without the requirement of a central network server.

**Social media**: forms of communication through which users create and share information, ideas, messages, and other content via the Internet.

**Spam**: bulk, unsolicited (junk) e-mail.

**Typosquatting**: a form of cybersquatting that relies on mistakes, such as typographical errors, made by Internet users when entering information into a Web browser.

[[return to top]](#_top)

# What's New in This Chapter

The following elements are improvements in this chapter from the previous edition:

* New chapter-opening scenario regarding a fake Facebook page that is disparaging and embarrassing--on online defamation or invasion of privacy
* 3 New Numbered Case Examples:
	+ on spam based on 2019 case
	+ on pirated movies and television based on a 2019 case
	+ on cookies and data collection based on a 2019 case
* New Ethical Issue: *What are the privacy implications of the facial recognition industry?*
* 1 New Numbered Example:
	+ on online defamation
* 1 New Case:
	+ *Campbell v. Facebook* (2020) – The court had to determine a remedy after Facebook confirmed that it collects the "content and other information" of its users when they "message or communicate with others."

[[return to top]](#_top)

# Chapter Outline

*In the outline below, each element includes references (in parentheses) to related content. “PPT Slide #” refers to the slide number in the PowerPoint deck for this chapter (provided in the PowerPoints section of the Instructor Resource Center). Introduce the chapter and review objectives for Chapter 08. (PPT Slide 3).*

1. **8-1 Internet Law** (PPT Slide 5-14)
	1. **Spam**
		1. The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act prohibits false and deceptive e-mails originating in the United States.
		2. The Federal CAN-SPAM Act
			1. **Case Example 8.1** Zoobuh
		3. The U.S. Safe Web Act allows U.S. authorities to cooperate and share information with foreign agencies in investigating and prosecuting those involved in spamming, spyware, and various Internet frauds and deceptions. The act includes a “safe harbor” for Internet service providers.
	2. **Domain Names**
		1. Trademark owners often use their mark as part of a domain name (Internet address). The Internet Corporation for Assigned Names and Numbers (ICANN) oversees the distribution of domain names.
	3. **Cybersquatting**
		1. Registering a domain name that is the same as, or confusingly similar to, the trademark of another and then offering to sell the domain name back to the trademark owner if known as cybersquatting. Anticybersquatting legislation makes this practice illegal if the one registering, trafficking in, or using the domain name has a “bad faith intent” to profit from that mark.
			1. **Example 8.2** Apple, Inc.
	4. **Meta Tags**
		1. Search engines compile their results by looking through a website’s meta tags, or key words. Using another’s trademark in a meta tag without the owner’s permission normally constitutes trademark infringement.
			1. **Case Example 8.5** Nespresso USA, Inc.
	5. **Trademark Dilution in the Online World**
		1. When a trademark is used online, without authorization, in a way that diminishes the distinctive quality of the nark, it constitutes trademark dilution. Unlike infringement actions, trademark dilution claims do not require proof that consumers are likely to be confused by a connection between unauthorized use and the mark.
	6. **Licensing**
		1. Many companies choose to permit others to use their trademarks and other intellectual property online through licensing. The purchase of software generally involves a license agreement. These agreements frequently include restrictions that prohibit licensees from sharing the file and using it to create similar software applications.
2. **8-2 Copyrights in Digital Information** (PPT Slides 15-23)
	1. ***Knowledge Check Video Activity (1) PPT Slide: 2 ½ minute(s) total (5 minutes with discussion and review of answer).*** *Tests students’ knowledge of Intellectual Property and social media. After answer is provided, review with students the issues that have arisen with social media and copyright how to address them.*
3. **Copyrighted Infringement**
	* 1. Much of the material on the Internet (including software and database information) is copyrighted. In order to that material to be transferred online, it much be “copied.” Generally, whenever a party downloads software or music without authorization, a copyright is infringed.
			1. **Spotlight Case Example 8.6** Stephanie Lenz
4. **File-Sharing Technology**
	* 1. When file-sharing is used to download others’ stored music files or illegally copied movies, copyright issues arise. Individuals who download music or movies in violation of copyright laws are liable for infringement. Companies that distribute file-sharing software or provide such services have been held liable for the copyright infringement of their users if the software or technology involved promoted copyright infringement.
			1. **Case Example 8.7** UN4 Productions, Inc.
5. **8-3 Social Media** (PPT Slides 24-27)
6. **Legal Issues**
	* 1. The emergence of Facebook and other social networking sites has had a number of effects on the legal process. Social media posts have had an impact on litigation and settle agreements. Law enforcement and administrative agencies now routinely use social media to detect illegal activities and conduct investigations, as do many businesses.
			1. **Case Example 8.9** Patrick Snay
			2. **Case Example 8.12** Jennifer O’Brien
			3. **Case Example 8.13** Virginia Rodriguez
7. **Protection of Social Media Passwords**
	* 1. Private employers and schools have sometimes looked at an individual’s Facebook or other social media account to see if it included controversial postings. A number of states have enacted legislation that protects individuals from having to divulge their social media passwords. Such laws may not be completely effective in preventing employers from rejecting applicants or terminating workers based on their social media postings.
8. **Company-wide Social Media Networks**
	* 1. Many companies today form their own internal social media networks through which employees can exchange messages about topics related to their work.
9. **8-4 Online Defamation** (PPT Slides 28-30)
10. **Identifying the Author of Online Defamation**
	* 1. Federal and state statutes apply to certain forms of cyber torts, or torts that occur in cyberspace, such as online defamation. Under the federal Communications Decency Act (CDA), Internet service providers generally are not liable for defamatory messages posted by their subscribers.
			1. **Case Example 8.15** Yelp, Inc.
	1. **Liability of Internet Service Providers**
		1. Under the CDA, ISPs usually are treated differently from publishers in print and other media, and are not liable for publishing defamatory statements that come from a third party. Although the courts generally have construed the CDA as providing a broad shield to protect ISPs from liability for third party content, some courts have started establishing limits to this immunity.
			1. **Case Example 8.16** Roommate.com
11. **8-5 Privacy** (PPT Slides 31-39)
12. **Reasonable Expectation of Privacy**
	* 1. Numerous Internet companies have been accused of violating users’ privacy rights. To sue for invasion of privacy, a person must have a reasonable expectation of privacy in the particular situation. It is often difficult to determine how much privacy can reasonably be expected on the Internet.
13. **Data Collection and Cookies**
	* 1. Whenever a consumer purchases items online from a retailer, the retailer collects information about the consumer through “cookies.” Consequently, retailers have gathered large amounts of data about individuals’ shopping habits. It is not always clear whether collecting such information violates a person’s right to privacy.
			1. **Case Example 8.17** Vizio, Inc.
14. **The Electronic Communications Privacy Act (ECPA)**
	* 1. The ECPA prohibits the intentional interception or disclosure of any wire, oral, or electronic communication.
			1. The ECPA includes a “business-extension exception” that permits employers to monitor employees” electronic communications made in the ordinary course of business (but not their personal communications).
			2. The Stored Communications Act (SCA) is part of the ECPA and prohibits intentional unauthorized access to stored electronic communications (such as backup data stored by an employer).
				1. **Case Example 8.18** Facebook
15. **Internet Companies’ Privacy Policies**
	* 1. Many companies establish Internet privacy policies, which typically inform users what types of data they are gathering and for what purposes it will be used.

[[return to top]](#_top)

# Discussion Questions

You can assign these questions several ways: in a discussion forum in your LMS; as whole-class discussions in person; or as a partner or group activity in class.

1. **Discussion – Internet Law (PPT Slides 5-14). Duration 20 Minutes.**
2. **Do Internet service providers (ISPs) have an ethical duty to advise their users if the information that the users provide for distribution through the ISPs might violate the law?**
	1. 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.
3. **Why is it important to protect trademarks from trademark dilution and cybersquatting?**
4. 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.
5. **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?**
6. 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.
7. **Why are ISPs exempt from liability, under some statutes, for the actions of their customers?**
8. Sometimes it is viewed as unfair to impost liability on an ISP for the actions of its customers, who may number in the hundreds of thousands, or more. It is 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.
9. **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 website?**
10. 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 website 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.
11. **Discussion – 8-2 Copyrights in Digital Information (PPT Slides 15-23). Duration 20 minutes.**
12. **Why is copyright law important in cyberspace?**
13. 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.
14. **How might a file-sharing system, or a similar service, be put to commercially significant but nonfringing uses?**
15. One possibility is that the service could pay copyright owners before allowing the transmission of their material via the Internet and charge its website’s users to down­load that material. The same might be done with other types of intellectual property—movies, books, etc.
16. **Discussion – 8-3 Social Media (PPT Slides 24-27). Duration 5 Minutes.**
17. **As social media becomes ever more pervasive, what can be expected to occur with respect to trademark disputes?**
18. 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.
19. **Are there creative works that can be shared or otherwise used by anyone without permission and without the payment of royalties?**
20. 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?
21. **Discussion – 8-4 Online Defamation (PPT Slides 28-30). Duration 5 minutes.**
22. **Considering the anonymous nature of the Internet, has defamation become an outdated legal concept?**
23. Each day in blogs around the world, statements are posted that constitute libel. However, the cost of tracking down the person who made the libelous statement is too high to justify bringing a suit against that person. 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.

[[return to top]](#_top)

# Additional Activities and Assignments

1. **MindTap** – Why Does Online Privacy Matter to Me?
	1. Online auto-graded activities connect the upcoming chapter to an authentic, real-world scenario designed to pick engagement and emphasize relevance. Consists of 1 multiple choice question in each.
2. **MindTap** – Learn It: Reasonable Expectation of Privacy on the Internet; Monitoring Employees’ Emails; Electronic Surveillance
	1. Online auto-graded activities that review foundational concepts presented in this chapter, and assesses students’ comprehension of the topics. Consists of 2 multiple choice questions in each.
3. **MindTap** – Check Your Understanding: Internet Law, Social Media, and Privacy
	1. Online auto-graded activity that assesses students’ foundational knowledge of the concepts presented in this chapter. Consists of 10 multiple choice questions.
4. **MindTap** – Case Problem Analysis: Internet Law
	1. Online auto-graded activity that first walks students through a fact pattern, and then asks them to answer similar questions with slight variations in the fact pattern. Consists of approximately 5 fill-in-the-blank questions.
5. **MindTap** – Brief Hypotheticals: Internet Law, Social Media, and Privacy
	1. Online auto-graded activity that presents 5 fact patterns in which students are asked to apply the concepts of the chapter, and to come up with a legal conclusion. Consists of 5 multiple choice questions.

[[return to top]](#_top)

# Additional Resources

## Cengage Video Resource

* MindTap Quick Lesson Video:
	+ Intellectual Property and Social Media. Duration 3:43 minutes.

[[return to top]](#_top)