Instructor’s Manual: Chapter 8

Ethical, Social, and Political Issues in E-commerce

**Learning Objectives**

After reading this chapter, your students should be able to:

* Understand why e-commerce raises ethical, social, and political issues.
* Understand basic concepts related to privacy and information rights, the practices of e-commerce companies that threaten privacy, and the different methods that can be used to protect online privacy.
* Understand the various forms of intellectual property and the challenges involved in protecting it.
* Understand how the Internet is governed and why taxation of e-commerce raises governance and jurisdiction issues.
* Identify major public safety and welfare issues raised by e-commerce.

# Key Terms

accountability, p. 510

anonymous information, p. 519

anonymous profiles, p. 522

Anticybersquatting Consumer Protection Act (ACPA), p. 554

copyright law, p. 543

cyberpiracy, p. 555

cybersquatting, p. 555

data image, p. 522

deep linking, p. 558

Digital Millennium Copyright Act (DMCA), p. 546

dilemma, p. 511

dilution, p. 554

doctrine of fair use, p. 544

due process, p. 510

ethics, p. 509

framing, p. 559

General Data Protection Regulation (GDPR), p. 532

governance, p. 560

information privacy, p. 513

informed consent, p. 526

liability, p. 510

linking, p. 558

net neutrality, p. 563

opt-in model, p. 526

opt-out model, p. 526

patent, p. 550

persistent location tracking, p. 525

personal profiles, p. 522

personally identifiable information (PII), p. 519

Privacy Shield, p. 533

privacy, p. 513

profiling, p. 522

responsibility, p. 510

right to be forgotten, p. 513

safe harbor, p. 532

trade secret, p. 559

trademark, p. 553

# Brief Chapter Outline

*The Right to be Forgotten: Europe Leads on Internet Privacy*

8.1 Understanding Ethical, Social, and Political Issues in E-commerce

A Model for Organizing the Issues

Basic Ethical Concepts: Responsibility, Accountability, and Liability

Analyzing Ethical Dilemmas

Candidate Ethical Principles

8.2 Privacy and Information Rights

What Is Privacy?

Privacy in the Public Sector: Privacy Rights of Citizens

Privacy in the Private Sector: Privacy Rights of Consumers

Privacy Protection as a Business

Privacy Advocacy Groups

Limitations on the Right to Privacy: Law Enforcement and Surveillance

*Insight on Technology: Apple: Defender of Privacy?*

8.3 Intellectual Property Rights

Types of Intellectual Property Protection

Copyright: The Problem of Perfect Copies and Encryption

Patents: Business Methods and Processes

Trademarks: Online Infringement and Dilution

Trade Secrets

Challenge: Balancing the Protection of Property with Other Values

8.4 Governance

Can the Internet Be Controlled?

Taxation

*Insight on Business: Internet Sales Tax Battle*

Net Neutrality

8.5 Public Safety and Welfare

Protecting Children

Cigarettes, Gambling, and Drugs: Is the Web Really Borderless?

*Insight on Society: The Internet Drug Bazaar*

8.6 Careers in E-commerce

8.7 Case Study: *The Pirate Bay: Searching for a Safe Haven*

8.8 Review

Key Concepts

Questions

Projects

References

# Figures

Figure 8.1 The Moral Dimensions of an Internet Society, p. 508

# Tables

Table 8.1 Unique Features of E-commerce Technology and Their Potential Ethical, Social, and/or Political Implications, p. 507

Table 8.2 The FTC’s Fair Information Practice Principles, p. 514

Table 8.3 Federal Privacy Laws Applicable to the U.S. Government, p. 516

Table 8.4 Privacy Laws Affecting Private Institutions, p. 517

Table 8.5 Personal Information Collected by E-commerce Sites, p. 519

Table 8.6 The Internet’s Major Information-Gathering Tools and Their Impact on Privacy, p. 520

Table 8.7 Internet Users’ Efforts to Preserve Privacy, p. 521

Table 8.8 The FTC’s New Privacy Framework, p. 527

Table 8.9, FTC Privacy Enforcement Actions, p. 528

Table 8.10 Criteria to Use When Examining Privacy Policies, p. 531

Table 8.11 Technological Protections for Online Privacy, p. 535

Table 8.12 Privacy Advocacy Groups, p. 536

Table 8.13 Fair Use Considerations to Copyright Protections, p. 544

Table 8.14 The Digital Millennium Copyright Act, p. 547

Table 8.15 Selected E-commerce Patents, p. 552

Table 8.16 Internet and Trademark Law Examples, p. 555

# Teaching Suggestions

This chapter summarizes the various ways that e-commerce and Internet technologies have raised serious social issues. More importantly, the chapter helps students learn about ethical, social, and political issues. Students should understand that successful business people take these issues to heart, and do so because good ethics is usually good business in the long term. On the other hand, it can sometimes be expensive to be good, or to do the right thing in the short term. Conversely, the costs of doing the wrong thing can be enormous. The consequences of potential litigation are potentially very negative for the business. In other cases, wise people seek out the ethical solutions to business problems simply because they personally have strong ethical convictions. Although each chapter contains information on social issues, this chapter aims to take a systematic look at relevant ethical principles, ethical analysis, and selected contemporary ethical issues raised by e-commerce.

Perhaps the greatest challenge in this chapter is to encourage students to think systematically in terms of ethical principles, laws, and acceptable behavior, rather than simply express their personal point of view. For example, many students may rationalize their downloading of copyrighted material as something theyfeel good about because “ethics is all relative,” and “everyone has their own sense of right or wrong.” They may also rationalize their behavior on the grounds that the people they steal from (variously, the record companies, the artists, and the promoters) are all rich. This personalized view of ethics fails to take into account the perceptions of customers, regulators, suppliers, employees, and business partners, as well as the long-term interests of shareholders. Other students may say, “As long as my business stays within the law, we are OK.” Once again, this view fails to recognize that trust and the perception, let alone the reality, of fairness demand a higher standard than the law. Customers often expect a higher standard of treatment than the minimal treatment required by law.

A second challenge is to convince students that ethical, social, and political awareness is an important part of business life. You should emphasize to your students that most employers do not want to hire employees who have no ethical convictions or who believe that business is a jungle where it is “every person for themselves.” Many job interviewers will seek to identify the ethical sensibility of potential recruits. Students should prepare for these questions. Ask your students if they, as an employer, would like to hire a person whom they felt had few moral or ethical scruples. Is a potential recruit who glorifies downloading “free” music from the Web more—or less—likely to download and use your firm’s intellectual property for his or her personal gain?

The opening case, *The Right to Be Forgotten: Europe Leads on Internet Privacy*, looks at the thorny question of privacy versus free speech on the Internet. There are many conflicting values involved. Questions for class discussion on this case might include the following:

* Is Google responsible for the accuracy of links to other information? Why or why not?
* Why do European and American views on privacy protection differ so dramatically?
* How can the different perspectives on privacy be managed in a global environment like the Internet?

## Key Points

*Understanding the Ethical, Social, and Political Issues in E-commerce.*Section 8.1 provides an overview of ethical, social, and political issues in e-commerce.A good place to start is Table 8.1, which illustrates how the unique features of e-commerce technology can also become ethical liabilities. Figure 8.1 succinctly identifies the key issues discussed in the chapter and attempts to illustrate the idea that the discussion will proceed on three levels: individual (ethical dilemmas), society (social choices), and policy (laws and regulation). Students should keep in mind that there is a connection among these levels: Laws reflect social choices, which in turn are based on fundamental ethical principles strongly held by individuals. Put another way, political debates reflect ethical debates.

The key terms to emphasize in this section are *responsibility*, *accountability*, *liability*,and *due process*. These are the bedrock concepts of all ethics.

One way to teach this section is to take a contemporary e-commerce story from the newspaper and analyze the ethical dilemmas. For instance, you might consider a story about file sharing networks encouraging the sharing of copyrighted content, such as movies or music. Have the students use the model proposed in this section to analyze the story. You might also ask them to consider alternative forms of delivery that are legal, satisfy demand, and are profitable, such as Netflix, Apple’s iTunes Music Store, or Pandora’s service. Finally, you might ask them to apply the seven ethical principles suggested in this section to any of the existing or potential future music delivery systems.

*Privacy and Information Rights.* Section 8.2 begins with a definition of privacy and information privacy, as well as the European “right to be forgotten,” which is discussed in further detail in the opening case. Table 8.2 describes the FTC’s Fair Information Practice (FIP) principles, which have been integral to the development of privacy protection in the United States. The section then distinguishes between privacy issues as they relate to the public sector versus privacy issues in the private sector (Table 8.3 provides a list of privacy laws applicable to the U.S. government, whereas Table 8.4 lists privacy laws affecting private institutions). Most of the remainder of the section focuses on the privacy rights of consumers. Table 8.5 provides a glimpse of what e-commerce sites collect directly from consumers. Key concepts are personally identifiable information (PII), anonymous information, and profiling. Table 8.6 identifies the ways various devices, applications, and tools can be used to gather user information and potentially violate privacy. The section then looks at some specific privacy issues posed by social networks and mobile devices, and then looks at various regulatory efforts by the FTC and the FCC to help ensure consumer privacy. One interesting assignment is to ask students to analyze the privacy policy of a website that they use, using the criteria set forth in Table 8.10. They may be surprised by what they find!

Students also usually find it interesting that Europeans in the EU (European Union) have a much stronger set of privacy laws than the United States. Be sure to spend some time explaining the EU approach to privacy protection, including the original 1998 Data Protection Directive and the new General Data Protection Regulation (GDPR that is scheduled to take full effect in May 2018.

It is also useful to explore with students the question of whether the industry can regulate itself, as it claims, using voluntary, industry-supported, and privacy seal programs, and various technological approaches to privacy protection. Also encourage students to visit the websites of one or more of the privacy advocacy groups listed in Table 8.12.

The *Insight on Technology* case, *Apple: Defender of Privacy?*, discusses the issues that arise when the right to privacy conflicts with government’s desire to surveil and monitor for law enforcement purposes. Class discussion questions might include the following:

* Are there circumstances that warrant the invasion of personal digital information and property?
* Do you think the All Writs Act of 1789 should be applicable to today’s technology-driven privacy issues?
* Should citizens charged with a crime or convicted criminals have any rights to privacy?
* How does Apple’s view on privacy differ from those of Facebook’s and Google’s?

*Intellectual Property Rights.*Section 8.3 defines intellectual property and describes the main ways society has chosen to protect intellectual property: copyright, patent, trademark, and trade secrets law.

In terms of copyright, the main distinction to get across to students is the difference between an idea and its expression. Copyright protects the expression, not the idea. Ideas and expression can merge so that some ideas can only have one expression; take Microsoft’s Windows and Apple’s version of Windows, for instance. The most important recent development in copyright is the Digital Millennium Copyright Act (DCMA). Two significant provisions in this act are the provision against breaking encryption codes that protect intellectual property and the “safe harbor” provided to ISPs and search engines that take down infringing content. Google has invoked the safe harbor provision in the lawsuit by Viacom with respect to YouTube videos.

Patents protect ideas for limited periods of time. The danger of patents is that they may stifle competition. Table 8.15 provides a list of selected e-commerce patents.

Trademarks help identify and distinguish goods in the marketplace; they play an important role in branding. E-commerce has created opportunities for mischievous behavior by violators of trademark. Table 8.16 provides a list of various Internet-related trademark issues and related legal cases.

Trade secrets law protects a kind of intellectual property that has to do with business procedures, formulas, and methods of manufacture and service delivery from which a firm derives value and does not want to share with others in the form of a patent or copyright application. Trade secrets are protected by both state, and now, with the enactment of the Defend Trade Secrets Act, federal law.

One way to conclude this discussion, after students understand the basic concepts of intellectual property, is to debate whether society would be better-off without intellectual property law. Intellectual property laws restrict the flow of ideas, music, and other forms of expression. On the other hand, these same laws incentivize people to create new expression.

*Governance Issues.*Section 8.4 examines various governance issues raised by e-commerce. During the early years of e-commerce, it was customary to think about the Internet as far too powerful, yet amorphous, for any government to control. We now know that the Internet—or at least the key players such as ISPs, e-commerce sites, and telecommunication carriers—can be controlled just as in other forms of media. One of the more interesting governance issues in the United States is taxation of online purchases. States and localities are pushing hard for a slice of the e-commerce business pie. The *Insight on Business* case, *Internet Sales Tax Battle*, takes a closer look at this issue. Questions for class discussion might include the following:

* Given the nature of the Internet, should sales tax be based on the location of the consumer rather than the seller?
* What are the different approaches Amazon has taken with respect to sales taxes?
* Are bricks-and-clicks retailers disadvantaged by local sales tax laws?

Net neutrality is another issue that has been in the news, with the FCC’s ruling in 2015 that Internet broadband service providers should be viewed as public utilities similar to telephone companies, and, therefore, regulated by the FCC to ensure fair access to all, deployment of acceptable broadband service levels, and competition among providers. However, the debate over net neutrality is not over, with the change in the White House following the election of Donald Trump, and the resignation of Thomas Wheeler, the FCC chairman, who has been a major proponent of net neutrality, so this is a topic you should be prepared to provide an update on.

*Public Safety and Welfare.*How could e-commerce affect public safety and welfare? Section 8.5 may, at first, puzzle most students. You can start by having students read and discuss the *Insight on Society* case, *The Internet Drug Bazaar*. You can use the following questions to spark class discussion:

* What’s wrong with buying prescription drugs online, especially if the prices are lower?
* What are the risks and benefits of online pharmacies?
* Should online pharmacies require a physician’s prescription?
* How do online pharmacies challenge the traditional business model of pharmacies and drug firms?
* What are the challenges in regulating online pharmacies?
* Who benefits and who loses from online pharmacies?

Drugs (both legitimate and illegitimate types), gambling, pornography, and cigarette sales are just a few areas where e-commerce raises public safety and welfare issues. Another interesting discussion might ensue if you have students come up with ways to control the Internet, so it is less of a threat.

In Section 8.6, we offer students information and tips about how the concepts they’ve learned in this chapter can help them prepare for an interview for an entry-level position as an e-commerce privacy research associate.

The chapter-ending case study, *The Pirate Bay: Searching for a Safe Haven*, in Section 8.7, is a fascinating example of the creative destruction of the traditional recorded music industry, the interplay of technology, law, popular culture, and politics, and the role of intellectual property on the Internet. There will be little difficulty obtaining student participation when you pose the following question: “Should file-sharing networks (or those who encourage sharing of copyrighted files) be allowed to distribute copyrighted music on the Web without having to compensate copyright holders?” Many students believe music should be free online even if this means: (a) ignoring claims by artists and record companies that they own the music, and (b) violating the law that protects the claims of copyright holders. On the other hand, paying for music has become acceptable again through the development of iTunes, subscription music services such as Spotify, smartphones, and cloud computing, where music is streamed, not downloaded. As cloud computing grows, downloading and “owning” music will be a thing of the past, as most music will be streamed to users connected to the Internet. It won’t be free, just convenient.

# Case Study Questions

1. *Why did TPB believe it was not violating copyright laws? What did the Swedish court rule?*

TPB claims it is merely a search engine providing pointers to existing P2P networks that it does not itself control. It says that it cannot control what content users ultimately find on those P2P networks, and that it is no different from any other search engine, such as Google or Bing, which are not held responsible for the content found on sites listed in search results. From a broader standpoint, TPB’s founders also claim that copyright laws in general unjustly interfere with the free flow of information on the Internet, and that in any event, they were not violating Swedish copyright law, which they felt should be the only law that applied. And they further claimed they did not encourage, incite, or enable illegal downloading.

The First Swedish Court in Stockholm declared TPB’s four founders guilty of violating Swedish copyright law, and sentenced each to one year in prison and payment of $3.5 million in restitution to the plaintiffs, all Swedish divisions of the major record firms (Warner Music, Sony, and EMI Group among them). The court found that the defendants had incited copyright infringement by providing a website with search functions, easy uploading and storage possibilities, and a tracker. The court also said that the four defendants had known that copyrighted material was shared with the help of their site and that the defendants were engaged in a commercial enterprise, the basis of which was encouraging visitors to violate the copyrights of owners. In fact, the primary purpose of TPB was to violate copyrights to make money for the owners (commercial intent).

*2. How has TPB managed to continue operating despite being found in violation of copyright laws?*

TPB appealed the court judgment, has not paid any fine, and its founders have, or are in the process of, serving jail sentences. TPB has dispersed multiple copies of its program to servers located in other countries. Although it has been hounded by lawsuits, police raids, and confiscation of servers in various countries, as well as having its top-level domains shut down in various countries, it has continued to operate by hopping from country to country.

*3. How has the music industry reacted to the problems created by pirates like TBP?*

The music industry has reacted by suing companies and individuals who it believes are involved in piracy, and encouraging strong government enforcement of copyright laws. In addition, the music industry has had to drastically change its business model and decisively move towards digital distribution platforms. They have made striking progress, and sales of music in a purely digital format now account for more revenue than sales of music in a physical format. To achieve this, the music industry has employed a number of different business models and online delivery platforms, including Apple’s iTunes pay-per-download model, subscription models, streaming models, and music in the cloud.

# End-of-Chapter Questions

1. *What basic assumptions does the study of ethics make about individuals?*

The study of ethics makes the basic assumption that individuals are free moral agents who are in a position to make choices.

1. *What are the basic principles of ethics?*

The basic principles of ethics are responsibility, accountability, liability, and due process. As free moral agents, individuals, organizations, and societies are responsible for the actions they take and should be held accountable to others for the consequences of those actions. Liability is a characteristic of political systems in which a body of law is in place so that accountability can be enforced. It permits individuals to recover damages for the actions of other individuals, systems, or organizations that cause them damage. Due process is a feature of law-governed societies and refers to a process in which laws are known and understood and there is an ability to appeal to higher authorities to ensure that the laws have been applied correctly.

1. *Explain Google’s position that YouTube does not violate the intellectual property rights of copyright owners.*

Google’s defense against accusations of copyright infringement rests upon the doctrine of fair use and the provision of the Digital Millennium Copyright Act (DMCA) of 1998. The doctrine of fair use permits limited use of copyrighted materials if certain conditions are met, such as the following:

* It does not harm the commercial value of the work.
* It is limited to very small portions.
* The nature of the work.
* The nature of use, e.g., non-commercial purpose.
* The context of use prevents seeking permission.

Google claims that YouTube meets at least some of these criteria. They also claim that it is sometimes impossible to know whether a video is infringing or not. Google also claims that it qualifies for the “safe harbor” provision of the DMCA, because YouTube promptly removes infringing content if it is requested to do so by copyright holders.

1. *Define universalism, slippery slope, the* New York Times *test, and the social contract rule as they apply to ethics.*

Universalism implies that if a solution is not correct for all situations, then it is not right for any specific situation. In simple terms, Immanuel Kant’s categorical imperative asks: If the rule were to be adopted in every case, would the organization or society survive?

The slippery slope rule states that if an action cannot be undertaken repeatedly, then it should not be taken at all. The solution might appear to work in one instance, but if the solution were repeated, negative outcomes might begin to occur, and in fact continue occurring at a pace that could not be stopped.

The *New York Times* test, or Perfect Information Rule, states that you must assume that the results of your decision on a matter will be the subject of the lead article in the *New York Times* the next day. In other words, if you would not want to see the reactions of your friends, family, and neighbors when they read about the results of your decision on the front page of the newspaper, then it is probably not the correct decision. Most criminals and other unethical actors operate under the assumption of imperfect information, meaning that they never expect to be exposed. When faced with an ethical dilemma, it is best to assume that perfect information will be available to all.

The social contract rule asks the decision maker to consider whether they would like to live in a society where the principle they are advocating was the organizing principle of the entire society.

1. *Explain why someone with a serious medical condition might be concerned about researching his or her condition online, through medical search engines or pharmaceutical sites, for example. What is one technology that could prevent one’s identity from being revealed?*

An individual with a serious medical condition might be concerned because in the United States there is no federal agency charged with enforcing privacy law. Private organizations and businesses can still use personally identifiable information gathered in commercial transactions for other business purposes. If a person with a serious medical condition were to purchase pharmaceuticals online for that illness, he/she would have cookies placed on his/her computer that would identify the person as a potential customer for other drugs for that illness. Because many companies do not even follow their own stated privacy policies, and opt-out procedures are usually difficult to find on a site, personal information or personal profiles might be sold or transferred to other companies, potentially even insurance companies. Advertising networks, or “profiling companies,” that have ads on the search engine site or pharmaceutical site may likely, without the person’s permission, place tags or identifiers on the person’s computer that will be used to track his/her movements as the person surfs the Web. In addition to collected behavioral information, a profile may contain inferential or psychographic data, information that the company infers about that person based on the sites they have visited.

The transition from fee-for-service health care to managed care has led to a demand for an unprecedented depth and breadth of personal information by a growing number of players, including health insurance companies. At the same time, the environment for information is moving rapidly from paper forms and files to electronic media, giving organizations a greater ability to tie formerly distinct information together, including data collected from the Web. The possibility of being dropped by an insurance company, not being able to transfer to a new insurance company along with new employment, or not being able to obtain health insurance at all, or of an employer finding out about a medical condition through the transfer of this data might be daunting. Therefore, as people become more aware that their movements on the Web are being tracked, they might become far less likely to explore sensitive topics such as personal medical conditions.

Some technologies that could prevent one’s identity from being revealed include anonymous surfing products and anonymous remailers.

1. *Name some of the personal information collected by websites about their visitors.*

Personal information that is collected by websites about their visitors includes the person’s e-mail address, postal address, and/or phone number. This is added to demographic data such as their age, occupation, income, education, gender, and ethnicity, and their behavioral data. Behavioral data includes: what websites they have visited (click-stream data), what purchases they have made (transaction data), and what preferences they have professed when filling out preference forms.E-commerce sites also collect bank account information, credit card account data, and sometimes the Social Security number and type of browser the customer uses.

1. *How does information collected through online forms differ from site transaction logs? Which potentially provides a more complete consumer profile?*

Transaction logs are anonymous information whereas online forms are personally identifiable information. The transaction log records an entry for each page a visitor views and each object they request. Online forms can be used to collect a variety of personal information about site visitors such as their name, address, e-mail address, and phone number. Online forms potentially provide a more complete consumer profile because this PII can be combined with the visitor-generated, click-stream behavior and other behavioral data to create a comprehensive personal profile.

1. *How is the opt-in model of informed consent different from opt-out? In which type of model does the consumer retain more control?*

In the opt-in model, the default behavior on the part of the website operator is *not* to approve the collection of data. In the opt-out model, the default is to automatically collect and use information unless otherwise notified. With the opt-in model, the consumer or site visitor must give consent before information about them can be collected and used. In the opt-out model, the consumer/site visitor must take an action to prevent the collection of data. The consumer retains more control in the opt-in model because no action to collect data will be undertaken unless they first agree to it. Only sites the consumer specifically requests to receive offers and promotions from will be allowed to collect data.

1. *What are the two core principles of the FTC’s Fair Information Practice Principles?*

The two core principles of the FTC’s Fair Information Practice Principles are notice/awareness and choice/consent. The FTC guidelines, which are not yet codified in law, recommend for the notice/awareness principle that sites disclose their information practices before collecting data. This includes identifying the data collector; all uses of the data; whether the data collection will be active or inactive, voluntary or required; the consequences of refusing to allow data to be collected; and the steps that will be taken to protect the confidentiality, integrity, and quality of the data. The choice/consent principle recommends that there be a choice system in place that allows consumers to choose how their information will be used for secondary purposes, other than supporting transactions. This includes internal uses by the collecting firm and transfer to third parties, and that opt-in/opt-out choices be made available.

*10. What is the Privacy Shield policy adopted by the European Union and the United States?*

On April 14, 2016, the European Parliament approved a new E.U. General Data Protection Regulation (GDPR) to replace the existing Data Protection Directive. The GDPR will take full effect throughout all E.U. member states on May 25, 2018. The GDPR applies across all E.U. countries, rather than the previous situation in which each member-state regulates privacy matters within its own borders. The GDPR applies to any firm operating in any E.U. country, requires unambiguous consent to use personal data for purposes like tracking individuals across the Web, limits the ability to use data for purposes other than those for which it was collected (tertiary uses, such as constructing user profiles), and strengthens the right to be forgotten, specifically, by allowing individuals to remove personal data from social platforms like Facebook, and prevent them from collecting any new information. Companies operating in the E.U. must delete personal information once it no longer serves the purpose for which it was collected. In addition, an independent ombudsman has been created to investigate complaints and enforce the policy. The GDPR has specific requirements with respect to the transfer of data outside of the E.U., one of which is that transfer is only allowed to countries that the E.U. deems as having adequate data protection laws. The United States is not considered to be one of those countries. As a result, after the previous safe harbor agreement that existed between Europe and the United States was struck down, it became necessary to negotiate a new agreement to enable E.U. citizens’ personal data to be transferred to the United States. This agreement, called the Privacy Shield, provides a way for participating companies to be considered in compliance with the E.U.’s data protection regulations. The Privacy Shield is more demanding than the previous safe harbor provisions and sets up additional monitoring and enforcement provisions.

*11. Name three ways online advertising networks have improved on, or added to, traditional offline marketing techniques.*

Online advertising networks now have the ability to precisely track not just consumer purchases, but also all browsing behavior on the Web. This can tell marketers much more about individual consumers than was previously known. For example, advertising networks can now compile information on all known interests of a consumer by collecting data on all content the viewer has accessed and all inclinations the consumer has expressed on preference forms. Advertising networks can also create the ability to dynamically adjust what the shopper sees on the screen. For instance, they can serve ads that conform to the inferences made from the collected data, and they can adjust the prices to conform to demographic or personal preference data. Furthermore, advertising networks create the ability to build and continually refresh these high-resolution data images or behavioral profiles of consumers. In summary, the scope and intensity of the data collection is strengthened to such an extent that merchants are now able to manipulate the shopping environment to their advantage.

*12. Explain how behavioral targeting is supposed to benefit both consumers and businesses.*

Behavioral targeting is supposed to benefit both consumers and businesses by allowing marketers to display ads that are more relevant to consumers. Businesses benefit by not paying for wasted advertising sent to consumers who have no interest in their product or service. The industry argues that by increasing the effectiveness of advertising, more advertising revenues go to the Internet, which in turn subsidizes free content on the Internet. Last, product designers and entrepreneurs benefit by sensing demand for new products and services by examining user searches and profiles.

*13. How could the Internet potentially change protection given to intellectual property? What capabilities make it more difficult to enforce intellectual property law?*

The Internet could potentially change the protection given to intellectual property because once a work becomes digital, it becomes much more difficult to control its access, use, distribution, and copying. Because digital media is so easy to replicate, transmit, and alter, unique challenges are presented. Theft is made much simpler in the digital world, and it becomes more and more difficult to establish the uniqueness of a work. It also becomes harder to enforce intellectual property law because the technology now exists to create perfect digital copies of various files including books, music, plays, poems, journal articles, and films. It is also simple to distribute these copies quickly, easily, and incredibly cheaply.

*14. What does the Digital Millennium Copyright Act (DMCA) attempt to do? Why was it enacted? What types of violations does it try to prevent?*

The Digital Millennium Copyright Act attempts to adjust copyright laws for the digital age. It was enacted when a confrontation erupted between the major copyright holders (the publishing, sheet music, record label, and commercial film industries), the providers of Internet content, users of copyrighted materials (libraries, universities), and the general consumer population. The act tries to prevent violations by imposing fines and possible imprisonment on hackers who attempt to break encryption schemes and distribute copyrighted materials worldwide. It also attempts to control the behavior of Internet Service Providers who often host infringing websites, or who provide Internet service to routine infringers. The ISPs do not believe that they should be held accountable, or specifically, that they should have to put their users under surveillance or invade their privacy because they are merely the message carriers.

The Digital Millennium Copyright Act makes it illegal to make, distribute, or use devices that circumvent the technology-based protections of copyrighted materials, and it also holds the ISPs responsible for infringers once they have been notified of these infringements. ISPs must immediately take down violating sites or be subject to prosecution themselves. Copyright owners can subpoena in federal court to obtain the personal identities of suspected violators from the ISP. ISPs must also inform all their subscribers of their copyright management policies. All provisions of the DMCA are designed to prevent the widespread online violation of copyright.

*15. Define cybersquatting. How is it different from cyberpiracy? What type of intellectual property violation does cybersquatting entail?*

Cybersquatting means registering, trafficking in, or using a domain name with the bad-faith intent to profit from a trademark belonging to someone else. It refers to the practice of buying domain names that reflect the names or trademarks of existing businesses intending to extort payments from the businesses. Cybersquatting is different from cyberpiracy because although cyberpiracy involves the same behavior, the intent is to divert traffic away from legitimate sites to infringing sites. It is a bad faith attempt to divert traffic that dilutes the value of the legitimate trademark. Cybersquatting is considered an intellectual property violation because the creator of the trademark or company name owns it according to the general principles of intellectual property law, which state that any tangible or intangible product of the human mind is protected from infringement.

*16. What is deep linking and why is it a trademark issue? Compare it to framing—how is it similar and different?*

Deep linking is the creation of a link to a page deep within another website using a publicly accessible HTML anchor tag. The home page of the target site is bypassed to access a page deep within that site. This becomes a trademark issue, for example, in the case of Ticketmaster versus Tickets.com. When Tickets.com did not have available tickets for a particular event, they would redirect users to a page deep within the Ticketmaster site to obtain those tickets. These customers might not ever realize that they were on a different site and that a different firm, indeed a direct competitor firm, was fulfilling their needs.

Framing on the other hand, is displaying the content of another website on your own site within a frame or window. The user never leaves the original site but can be exposed to advertising that is not that of the content owner. Framing may trigger a dispute under copyright and trademark law theories because a framed site can alter the appearance of the content and create the impression that its owner endorses or voluntarily chooses to associate with the framer. It can also divert advertising revenue from the content owner’s site. It is similar to deep linking in that the site visitor is accessing content from another site, but it is different in that with framing, the site visitor never even clicks a link to leave the site.

*17. What are some of the tactics businesses that are illegal in the United States use to operate outside the law on the Internet?*

The main tactic that businesses that are illegal in the United Sates use to operate outside of the law on the Internet is operating from offshore sites, for example, in Antigua or Costa Rica, so as to operate beyond the jurisdiction of the state and federal prosecutors.

*18. Why can’t pornographic sites simply be banned in the United States? Why has the Supreme Court struck down legislation intended to protect children from pornography?*

Courts have ruled that banning pornographic sites violates the First Amendment protections of freedom of speech, and second, defining pornography is difficult. Proscribing pornography may result in some legitimate works of art being banned.

*19. What is the “right to be forgotten”? What are some of the risks and benefits of establishing this right?*

The right to be forgotten is a claim that individuals should be able to access, edit, and change or delete personal information about them that has been collected by any website. There are limits on this right having to do with the public’s interest in criminal records, and the records of public figures. The benefit is that ordinary people can have inaccurate, old, or irrelevant information removed from their Internet record. The risk is that criminals will be able to hide their past and pose a risk to the public.

*20. What is the doctrine of “fair use”? Why did the courts decide that Google’s scanning of copyrighted books was a “fair use”?*

The doctrine of fair use allows copyrighted material to be used without permission of the copyright holder under certain circumstances. These are: character of use, nature of the work, amount of work used, market effect of use, and context of the use. Courts have concluded that Google’s scanning of copyright books was a fair use because the project had a broad public purpose of making it easier for students, researchers, teachers, and the general public to find books, while also preserving consideration for author and publisher rights. The Google project was “transformative” in the court’s view, giving books a new character and purpose, making it easier to discover old books, and leading to increased sales.

**Projects**

1. *Go to Google and find the Advanced Search link. Examine its SafeSearch filtering options. Surf the Web in search of content that could be considered objectionable for children using each of the options. What are the pros and cons of such restrictions? Are there terms that could be considered inappropriate to the filtering software but be approved by parents? Name five questionable terms. Prepare a brief presentation to report on your experiences and to explain the positive and negative aspects of such filtering software.*

Google’s SafeSearch filter screens for sites that contain explicit sexual content and deletes them from its search results. No filtering turns off SafeSearch filtering completely. The advantage of such filtering is that it prevents children from being exposed to material that parents deem unsuitable. The disadvantage of such filtering is that in some circumstances it may filter content that has educational value. It is also possible that there might be search terms considered potentially inappropriate by Google’s filter, but not by some parents.

1. *Develop a list of privacy protection features that should be present if a website is serious about protecting privacy. Then, visit at least four well-known websites and examine their privacy policies. Write a report that rates each of the websites on the criteria you have developed.*

Student lists of privacy protection features may vary somewhat but will likely follow the FTC’s FIP (Fair Information Practice) Principles as well as their profiling recommendations:

* Consumers must receive notice of network advertisers’ profiling activities on host websites and have the ability to choose not to participate in profiling.
* Clear notification of data collection must be given before it begins for personally identifiable information. Consumers must opt-in before data collection can begin.
* Clear and conspicuous notice must be given when non-personally identifiable information (or “clickstream” data) is collected for profiling. Consumers can opt-out of data collection.
* Once informed about the network advertiser’s information collection practices, consumers must be able to decide whether to participate in profiling.
* Reasonable access must be granted to personally identifiable information and other information that is associated with it to allow for inspection and correction.
* Sites are required to make reasonable efforts to protect the data they collect for profiling purposes from loss, misuse, alteration, destruction, or improper access.
* Enforcement must be done by third parties such as seal programs and accounting firms.
* No collection of sensitive data is permitted at all. This includes sensitive financial, medical, sexual behavior or orientation information, and Social Security numbers.
* Selling or renting of data to third parties is prohibited.
* Customers’ credit card data can only be transferred over secured connections.

1. *Review the provisions of the Digital Millennium Copyright Act of 1998. Examine each of the major sections of the legislation and make a list of the protections afforded property owners and users of copyrighted material. Do you believe this legislation balances the interests of owners and users appropriately? Do you have suggestions for strengthening “fair use” provisions in this legislation?*

Although the DMCA has six sections, Title I and Title II are the two most relevant. Title I of the DMCA protects the rights of property owners by creating two new prohibitions: one on the circumvention of technological measures used by copyright owners to protect their works, and the other on tampering with copyright management information.

Section 1201 of Title I divides technological measures into two categories: measures that prevent unauthorized access to a copyright work and measures that prevent unauthorized copying of a copyrighted work.

Circumventing measures put into place to prevent unauthorized access is prohibited. However, Section 1201 includes a number of exceptions to this rule. For instance, non-profit library, archival, and educational institutions are not prohibited from circumventing solely for making a good faith determination as to whether they wish to obtain authorized access to the work. There are also exceptions for reverse engineering for the purpose of identifying and analyzing elements of a computer program necessary to achieve interoperability with other programs, for encryption research, for protection of minors (allows a court applying the prohibition to a component or part to consider the necessity of its incorporation in technology that prevents access of minors to material on the Internet), for privacy protection (when the technological measure or the work it protects is capable of collection or disseminating personally identifying information about the online activities of a person), and for security testing.

Circumventing measures that prevent unauthorized copying is not prohibited, to assure that the public will have the continued ability to make fair use of copyrighted works. Making or selling devices that are used to circumvent either category is prohibited, however.

Section 1202 of Title I addresses the integrity of copyright management information (CMI), which is defined as: identifying information about the work, the author, the copyright owner, etc. This section protects copyright owners by prohibiting the knowing provision or distribution of false CMI, if done with the intent to induce, enable, facilitate, or conceal infringement. It bars the intentional removal or alteration of CMI without proper authority, as well as the dissemination of CMI or copies of works. Liability under subsection (b) requires that the act be done with knowledge or for civil remedies with reasonable grounds to know that it will induce, enable, facilitate, or conceal an infringement.

Section 1203 of Title I provides for civil remedies payable to injured parties, while Section 1204 provides criminal penalties of up to a $500,000 fine or 5 years imprisonment for a first offense, and up to a $1,000,000 fine or up to 10 years imprisonment for a subsequent offense.

Title II of the DCMA adds a new section to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. The limitations are for:

* Transitory communications: This is where the service provider merely acts as a data conduit, transmitting digital information from one point on a network to another at someone else’s request.
* System caching: This is the practice of retaining copies, for a limited time, of material that has been made available online by a person other than the provider, and then transmitted to a subscriber at his or her direction.
* Infringing material on websites or other information repositories hosted on service providers’ systems. To be eligible for this limitation, the provider must not have knowledge of the infringing activity, it must not receive a financial benefit directly attributable to the infringing activity, and upon receiving notification of claimed infringement it must expeditiously take down or block access to the material. (The service provider must promptly notify the subscriber that it has removed or disabled access to the material, and provide the subscriber with the opportunity to object.)

The service provider must also have filed with the Copyright Office a designation of an agent to receive notification of claimed infringement. To be eligible for any of the limitations, a service provider must:

* Adopt and reasonably implement a policy of termination in appropriate circumstances the accounts of subscribers who are repeat infringers.
* Accommodate and not interfere with “standard technical measures.”

The fourth limitation relates to hyperlinks, online directories, search engines, and the like. It limits liability for the acts of referring or linking users to a site that contains infringing material by using such information location tools, with the same eligibility requirements as for the third limitation. Although these provisions appear to offer more protection to the service providers than copyright owners, they are actually a strong tool for copyright owners because they provide a mechanism by which copyright owners can force service providers to block access to or remove infringing material.

Students can be expected to take varying positions as to whether the DMCA appropriately balances the interests of owners and copyright users. Some might note that the provisions of the DMCA can be used in such a way as to chill free speech. Others might argue that the DMCA does not go far enough and provides so many exceptions that it is not as strong a deterrent as it might be.

In terms of strengthening the “fair use” provisions, in some cases, encryption schemes work to prevent “fair use” that would otherwise be legal. One possible suggestion would be to require copyright owners who choose to protect their works through technological measures, to provide a means by which fair use can occur.

1. *Visit at least four websites that take a position on e-commerce taxation, beginning with the National Conference of State Legislatures (NCSL.org) and the National Governor’s Association (NGA.org). You might also include national associations of local businesses or citizen groups opposed to e-commerce taxation. Develop a reasoned argument for, or against, taxation of e-commerce.*

# Both the NCSL and the NGA are proponents of Internet taxation. Another website that students might visit for more views from proponents of Internet taxation is Streamlinedsalestax.org. Organizations opposing Internet taxation include the National Taxpayers Union (NTU.org) and Citizens Against Government Waste (CAGW.org), among others.

Arguments in favor of taxation of e-commerce might include the following:

* Legal: State governments have a constitutional right to levy and collect taxes on goods and services sold within the state. A federal law that bans taxation on Internet sales would be unconstitutional.
* Economic: Given the growth of e-commerce, if state and local governments are unable to collect sales taxes on online sales, they will lose a great deal of revenue. The loss of this revenue will result in an increase in the rate of other taxes, reduced services, and/or greater reliance on the federal government.
* Fairness: It is inherently unfair to traditional retailers who must collect sales taxes for Internet sales to remain untaxed. Doing so favors Internet retailers and places traditional retailers at a competitive disadvantage.

Arguments against taxation of e-commerce might include the following:

* Imposing state and local taxes on e-commerce will threaten the growth of e-commerce at a critical stage of development.
* The existing U.S. tax system is too complex and burdensome; it would be almost impossible for e-commerce companies to comply with the thousands of differing state and local tax rates. The sales tax burden from multiple jurisdictions that might have authority to levy taxes would be very high.
* Taxing e-commerce might drive e-commerce companies, many of which do not need to operate within the United States, to other locations.
* E-commerce stimulates purchases at retail stores and through catalogs, upon which taxes may already be collected.

**Companion Website, Learning Tracks, and Video Cases**

You can also direct your students to the Companion Website for the book, located at [www.e-commerce2018.com](http://www.e-commerce2018.com). There they will find a collection of additional projects and exercises for each chapter; links to various technology tutorials; information on how to build a business plan and revenue models; information on careers in e-commerce, and more. Learning Tracks that provide additional coverage of various topics and a collection of video cases that integrate short videos, supporting case study material, and case study questions are also available for download from the book’s Online Instructor Resource Center at [www.pearsonhighered.com/irc](http://www.pearsonhighered.com/laudon). Video Cases for this chapter include:

* Video Case 8.1 The Right to Be Forgotten
* Video Case 8.2 Facebook Privacy
* Video Case 8.3 What Net Neutrality Means for You