CHAPTER

9

Regulating Commerce and Speech in Cyberspace

LEARNING OBJECTIVES

Upon completing this chapter, you will successfully be able to:

- Differentiate and explain the relevance of key questions, concepts, and categories at the core of *Internet regulation*,
- Understand digital rights management (DRM) technology and explain why it is controversial from the perspective of regulating cyberspace,
- Describe the different kinds of regulation-related challenges posed by e-mail spam and assess the different kinds of arguments that have been advanced to show why spam is morally objectionable,
- Explain the difficulties involved in balancing free speech and censorship in online contexts and forums,
- Describe the difficulties involved in framing online pornography laws that will adequately protect children and evaluate the arguments that have been advanced to restrict and to abolish online pornography,
- Differentiate between online hate speech and online speech that can cause physical harm to others,
- Understand what is meant by "network neutrality," and explain how the outcome of the network neutrality debate will likely affect the future of the Internet.

In this chapter, we examine a wide range of issues and controversies that have led to a call for strong regulatory proposals in cyberspace. We begin our analysis with a scenario that briefly describes a recent incident involving two highly controversial organizations.

▶ SCENARIO 9–1: *Anonymous* and the Ku Klux Klan

The "Anonymous" group is an international network of hackers and hacktivists who have gained notoriety by disrupting governmental and commercial Web sites to make political statements and/or advance political causes. (Recall our earlier discussions of controversial aspects of Anonymous in Chapters 6 and 8.) In November 2014, Anonymous targeted the Ku Klux Klan (KKK) when that controversial group threatened protestors in Ferguson, Missouri (following an incident in which Michael Brown, a young black man, was shot dead by a white police officer). Some members of Anonymous hacked into two KKK Twitter accounts, and others launched cyberattacks against the Web sites of white supremacist groups that Anonymous

believed to be either sympathetic to or affiliated with the KKK. Following these attacks, Anonymous also made public the names of specific individuals it believed to be KKK members.[1] ■

Was Anonymous justified in carrying out these cyber-related attacks against the KKK? Should some form of Internet regulation that bans groups like the KKK from conducting racist online activities have been in place beforehand? On the one hand, many of the KKK's activities, as well as those of other white supremacist groups, are protected by free speech, whether their activities are carried out in physical space or in cyberspace. On the other hand, these kinds of groups also engage in a form of speech that "can cause physical harm to others." The latter kind of speech, as we shall see, is not clearly protected. But who, if anyone, is responsible for regulating the Internet with regard to both kinds of speech?

In the case involving the KKK and Ferguson protestors, Anonymous decided to intervene in a way that was not officially sanctioned by any existing laws. Furthermore, Anonymous' tactics in this incident clearly violated the law, since (as we saw in Chapters 6 and 7) acts of hacking and hacktivism are illegal. (And, in this case at least, it is not clear that "two wrongs make a right"!) The Anonymous–KKK scenario not only illustrates why Internet regulation is so controversial but also suggests how one's political ideology can influence his or her beliefs about which forms of online speech should be regulated and which should not.

The purpose of Scenario 9–1 was not to offer a resolution to the thorny issues underlying the Anonymous–KKK controversy, but to get us to begin thinking about some reasons why clearer and more explicit Internet regulation might be needed. Other cases and scenarios also could have been used to illustrate some of the reasons why many believe that stronger regulatory frameworks could help make the Internet a safer place. Consider, for example, the case of Tyler Clementi, an 18-year-old student at Rutgers University who committed suicide in 2010, following a cyber-related incident that received international attention. Clementi's roommate, Dharun Ravi, had secretly set up a Web cam(era) in their dorm room that exposed Clementi in a romantic encounter with a male student. Ravi was never formally charged in Clementi's suicide/death, but the incident raised questions about whether explicit regulatory schemes were needed to prevent a user's making a video of someone's activities publicly available on the Web without first getting that person's consent. So, we can begin to see why arguments for stronger regulation on the Internet have been advanced.

Disputes about whether and how to regulate cyberspace are hardly new; in fact, they have been going on at some level since the inception of the Internet itself. In this chapter, we will see that many conservative organizations have argued for regulatory schemes in the form of censorship of certain kinds of speech in cyberspace. Some liberal groups, on the contrary, who oppose any restrictions on free speech in cyberspace, argue that e-commerce, not speech, needs to be regulated.

For our purposes, regulatory concerns affecting "speech" will include issues involving pornography and hate speech, while e-commerce regulation issues include concerns affecting e-mail spam and digital rights management (DRM). With respect to the latter, we will also see why many are now concerned about a kind of cyberspace regulation that can be enforced via technology itself, that is, by means of "regulation by code" (which is exacerbated by DRM technologies). Some critics worry that regulation by code is becoming the default regulatory scheme in cyberspace. Before examining specific topics, however, we first consider some conceptual distinctions and clarifications that can better inform both our understanding and analysis of Internet regulation.

▶ 9.1 INTRODUCTION AND BACKGROUND ISSUES: SOME KEY QUESTIONS AND CRITICAL DISTINCTIONS AFFECTING INTERNET REGULATION

Weckert (2007) suggests that when discussing cyberspace regulation, we need to ask two separate questions:

1. *Can* it be regulated?

2. *Should* it be regulated?

Asking question (1) implies that it is not clear whether cyberspace can be effectively regulated. In this chapter, we will operate on the assumption that it can, in fact, be regulated. However, we acknowledge that regulation schemes can be difficult to implement and enforce, and we concede that regulation can have undesirable side effects in terms of both cost and efficiency.

Our main focus is on question (2), that is, the normative question as to whether cyberspace *ought* to be regulated. This question, as Weckert points out, can also be broken down into two separate questions. For example, we can ask whether the Internet should be "regulated in general" or whether it should be "regulated in any one country in the absence of cooperation by others."[2] In a later section of this chapter, we examine some controversies affecting consensus at the international level with regard to regulatory schemes and practices.

Despite some of the challenges that arise in the various schemes proposed for regulating cyberspace, Weckert and Al-Saggaf (2008) note that we should not presume against Internet regulation. In fact, they believe that a "strong moral case" can be made for regulating the Internet's content.[3] Others have suggested that a similar case can be made for regulating commerce in cyberspace. Before examining specific issues affecting the regulation of cyberspace, however, it is useful to consider two additional questions:

a. What do we mean by *cyberspace*?

b. What do we mean by *regulation*, particularly as it applies to cyberspace?

We postpone our analysis of (b) until Section 9.1.2. In answering (a), we first consider whether cyberspace is an actual "place" or whether it is best understood as a medium of some sort.

9.1.1 Is Cyberspace a Medium or a Place?

In Chapter 1, we loosely defined the Internet as the network of interconnected computers and devices, and we suggested that the terms "Internet" and "cyberspace" were roughly equivalent. In this chapter, we use the two terms interchangeably. But we have not yet described the ontology of cyberspace, that is, we have not said what, exactly, cyberspace *is*. For example, is it a *place*, that is, a virtual space that consists of all the data and information that resides in the connected servers and databases that make up the Internet? Or is cyberspace a (relatively new) *medium*?

Some believe that the Internet is best understood as a new kind of medium, significantly different from earlier media, such as the telephone or television. Whereas the telephone is a "one-to-one medium" and television is a "one-to-many medium," Goodwin (1995, 2003) describes the Internet as a "many-to-many medium." He also notes that one does not need to be wealthy to have access to this medium; nor does one need to win the approval of an editor or a publisher to speak his or her mind there. But should the Internet be viewed as a medium, or can it be better understood as a public space? Camp and Chien (2000) argue for the latter view.

Camp and Chien differentiate four types of media: *publisher*, *broadcast*, *distributor*, and *common carrier*. An example of a publisher is a newspaper or a magazine, and broadcast media include television and radio. Telephone companies and cable companies are instances of common carriers, conduits for the distribution of information. Camp and Chien argue that none of the media models are appropriate for understanding the Internet. Instead, they believe that a spatial model—one in which cyberspace is viewed as a public space with certain digital characteristics—is more plausible.

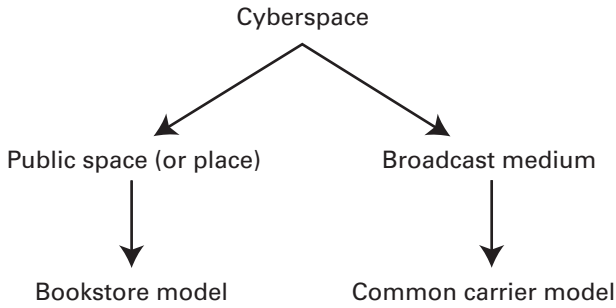

Figure 9-1 The ontology of cyberspace.

But can we model the Internet accurately as a public space, as Camp and Chien suggest? Or is it better understood as a new kind of *medium*, as Goodwin and others have argued? We are making more than a mere semantic distinction, because, as Camp and Chien point out, the model we use can influence our decisions about public policies on the Internet. If the Internet is viewed as a public space, for example, then there are good legal and moral reasons for ensuring that everyone has access to it. The ontology of cyberspace will ultimately determine whether and how we should (or perhaps should not) regulate it.

Consider the rules used to regulate the distribution and sale of "adult" magazines and videos in physical space. Bookstores and video rental stores are permitted to carry and sell such merchandise, and because a store is a physical place, certain sections can be partitioned so that adults can visit them but individuals under a certain age cannot. The rules are drastically different, however, for broadcast media such as television, where the Federal Communications Commission (FCC) regulates which kinds of content can be broadcast over the airwaves. Movies that can be rented and sold only to adults in stores can also be deemed inappropriate (by the FCC) for general television viewers. So before we can successfully resolve questions about Internet regulation, we need to keep in mind that the model we use to understand cyberspace will also strongly influence which regulatory schemes are appropriate.

Figure 9-1 illustrates our two models of cyberspace.

9.1.2 Two Categories of Cyberspace Regulation: Regulating Content and Regulating Process

To "regulate" means to monitor or control a product, process, or set of behaviors according to certain requirements, standards, or protocols. Sometimes regulatory discussions about cyberspace have centered on its *content*, for example, whether online pornography and hate speech should be censored. And sometimes the regulatory discussions have focused on which kinds of processes, that is, rules and policies, should be implemented and enforced in commercial transactions in cyberspace. Physical space is regulated in both ways.

Some regulatory agencies monitor the content, and others the process, of items in physical space. The Food and Drug Administration (FDA) monitors food products on the shelves of supermarkets to ensure that they meet health and nutrition standards; FDA regulations ensure that the contents of each food item both match and are accurately described by its label. Unlike the FDA, state public health boards do not regulate content; their regulations apply to conditions for compliance with community health standards. For example, public health officials inspect restaurants and grocery stores to ensure that they meet sanitation standards in their preparation and sale of food. So, an agency can regulate for content or process, or both.

In the commerce sector, federal and state agencies, such as the Federal Trade Commission (FTC) and the Security and Exchange Commission (SEC), enforce laws and policies that

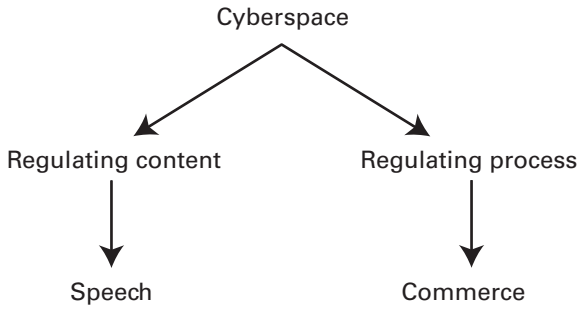

Figure 9-2 Two categories of cyberspace regulation.

apply to commercial activities and transactions; for example, they regulate against monopolies and other unfair business practices, such as those alleged in the Microsoft antitrust case in the late 1990s. Regulatory principles in the commerce sector also determine whether to permit mergers, such as the one between America Online (AOL) and Time Warner.

Figure 9-2 illustrates the ways in which cyberspace can be regulated.

It is not difficult to point out the positive effects that regulatory practices in physical space have for health and safety. Consider, for example, the role that state liquor boards (in the U.S.) play in regulating the distribution and sale of liquor: They determine who is and is not eligible for a license to distribute liquor in their state, and if a board determines that a licensed distributor has violated its licensing agreement with the state, its license can be revoked. And boards that regulate liquor can help to keep liquor out of the hands of minors and help to discourage an underground, or black, market for the sale of "bootleg liquor," which is not tested and certified as meeting standards of quality and authenticity. State liquor boards also help determine fair pricing to prevent unscrupulous merchants from price gouging. So, there are many good reasons for regulating the distribution and sale of liquor. But how can we extend this analogy to the Internet?

First, we can ask how we can possibly regulate cyberspace, which is inherently decentralized. Cyberspace is not compartmentalized neatly into state jurisdictions that can set up their own control boards. Does this mean that effective regulation of any type is impossible in cyberspace? Not according to Lessig (2000) and Agre (2005), who suggest that a decentralized cyberspace does not preclude Internet regulation from being carried out quite effectively. In describing the architecture of P2P (peer-to-peer) networks in cyberspace, Agre notes that decentralized institutions do not imply decentralized architectures, and vice versa. Lessig believes that in cyberspace, understanding architecture, or what he calls *code*, is the key to understanding how regulation works.

9.1.3 Four Modes of Regulation: The Lessig Model

Lessig describes four distinct but interdependent constraints, which he calls "modalities," for regulating behavior: *laws*, social *norms*, *market* pressures, and *architecture*. Before we apply each modality to cyberspace, consider how each can be applied in regulating behaviors in the physical world.

Cigarette smoking can be regulated through the passage and enforcement of explicit laws that make it illegal to smoke in public buildings. And we have specific laws that prohibit cigarette manufacturers from advertising on television or in magazines targeted at teenage audiences. Independent of explicit laws, however, social norms can also discourage cigarette smoking in public; for example, it is socially acceptable for homeowners to place "Thank you for not smoking in our house" signs on their front doors. And hotel

owners and operators can, under social pressure from prospective guests, partition smoking and nonsmoking rooms and sections of their establishments even if there is no explicit law requiring them to do so.

Market pressures can also affect smoking behavior. Cigarettes can be priced so that only the wealthiest people can afford to buy them. Finally, merchants can impose an "architecture of control" on cigarettes by using physical constraints. All cigarettes sold in grocery stores could be located behind locked doors, causing interruptions in checkout transactions. A cashier might have to temporarily suspend the transaction, locate the store's manager, and get the proper authorization and the key to open the locked doors to remove the cigarettes. Contrast this architecture with one in which cigarettes are available in vending machines easily accessible to everyone, including minors.

To apply Lessig's fourfold distinction to cyberspace, we replace architecture, which is in physical or geographic space, with *code*. Code, for Lessig, consists of programs, devices, and protocols—that is, the sum total of the software and hardware—that constitute cyberspace. Like physical architecture in geographic space, code sets the terms upon which one can enter or exit cyberspace. Also like architecture, code is not optional. Lessig notes that we do not choose to obey the structures that architecture establishes. Just as we are subject to architectures of physical space, so we are subject to code in cyberspace; a physical door can block you from entering a physical building, and a password requirement can prevent your entering a Web site. And code can be used to limit access to Web sites by requiring that users accept cookies (see Chapter 5) if they wish to visit those sites. Lessig believes that code can either facilitate or deter access to, or transfer of, information in cyberspace.

In Chapter 1, we saw that Moor (2007) described computer technology as "logically malleable" because, unlike most other technologies that are dedicated to performing specific tasks, computers can be instructed through software to perform an indefinite number of diverse functions. Lessig (2004) also illustrates an aspect of this technology's malleability, describing how different computer architectures create very different kinds of environments. He draws an interesting comparison between early and present-day computer networks, noting that whereas the Internet of 1995 (or what he calls "NET 95") had a "libertarian architecture," current networks do not.

To illustrate differences between these two architectures, Lessig compares the computer network systems at the University of Chicago and Harvard University in the late 1990s. During that period, the University of Chicago's network was still like NET 95, because anyone could connect his or her machine directly to (phone) jacks on the campus. As such, the code at Chicago favored freedom, or free speech. At Harvard, on the other hand, one first had to register his or her machine before getting on to the Harvard's network. Once registered, all interactions with the network could be monitored and identified by Harvard's network administrators. Lessig points out that at the University of Chicago, "facilitating access" had been the ideal (at that time); at Harvard, on the contrary, "controlling access" was (and still is) the ideal.

Note that the underlying network protocols (i.e., TCP/IP) were the same for the computer systems at both Harvard University and the University of Chicago. But layered on top of Harvard's TCP/IP protocol was an additional set of protocols, or *code*, which, Lessig argues, "facilitates control." Why should we care about the differences between the two kinds of architectures? Lessig points out that in the NET 95 environment, one could roam the Internet freely and anonymously. Today, one cannot. Lessig concludes from this that we have moved from what was once an "architecture of freedom" to an "architecture of control." He also concludes that in cyberspace, code is a more effective regulator than law. In fact, Lessig claims that in cyberspace, *code is the law*.[4]

► 9.2 DIGITAL RIGHTS MANAGEMENT (DRM)

To understand the force of Lessig's claim that (software) code is law, consider the role that "code" in the form of DRM tools plays in regulating digital media. DRM technologies allow content owners to regulate the flow of digital information by blocking access to it via "digital locks" supported by encryption mechanisms. The combination of DRM technology and copyright protection laws, such as the Digital Millennium Copyright Act (DMCA), makes it possible for the regulation and enforcement of policies and laws in cyberspace to a degree that never existed in the physical realm. DRM also makes it possible for corporations to make up new copyright-related rules and to enforce those rules via their own technologies and tools.

How is it possible for corporations to do this? First consider that, as Doctorow (2014) points out, there is no copyright law stating that it is illegal to skip through "piracy warnings" when viewing a movie on a DVD player. But suppose a viewer wishes to bypass or fast-forward through those warnings, as well as through a series of advertisements, displayed prior to the start of the movie. In this case, the viewer would likely have to break a "digital lock" (on the DVD player) to skip these segments of the DVD. But breaking that lock would violate DMCA's anticircumvention clause. (As we saw in Chapter 8, any program or device that circumvents DRM controls is in violation of Section 1201 of the DMCA.) Because the DMCA makes it illegal for someone to "descramble" a movie without permission, the (code that makes possible the) digital lock on the DVD player serves the same regulatory function as law (even where no explicit law exists). And because DMCA prohibits the development and use of technologies that could circumvent copyright management systems, it works hand in hand with DRM technology to control access to significant amounts of information now in digitized form.

9.2.1 Some Implications of DRM for Public Policy Debates Affecting Copyright Law

Critics worry about the many ways in which DRM technology can be used to enforce copyright law. Because software code in DRM systems is being developed and used with the express purpose of precluding the possibility of copyright infringement, Elkin-Koren (2000) fears that the traditional mechanism for debating public policy may now be closed to us. She notes that if the manufacturers of digital devices can decide what the copyright rules should be and if they are permitted to embed code in their products that enforces those rules, then there is no longer a need for, or even the possibility of, public policy debate about copyright issues.

Elkin-Koren notes that in the past, when individuals duplicated proprietary information by using the latest available technologies, we were often forced to question the viability of existing copyright laws in light of those new technologies vis-à-vis principles such as fair use (described in Chapter 8). She also notes that we could then engage in meaningful public policy debates about whether traditional copyright laws should apply or whether some new laws are needed. Thus we were able to challenge the viability and constitutionality of such laws through the judicial process.

However, Elkin-Koren worries that a framework for *balancing* the interests of individuals and the public, which in the past had been supported by "spirited policy debates" and judicial review, will no longer be possible in a world in which copyright policies are predetermined by code. As Spinello (2003) notes, restrictions embedded into computer code end up having the force of law without the checks and balances provided by the legal system. And Elkin-Koren argues that because of the technological controls embedded in software code (such as in DRM systems), our policies affecting information and digital media are becoming increasingly *privatized*. She also suggests that this trend toward privatization has enabled software companies to design code that reflects their own interests and values, without having to worry about any adverse effects that code can have for the public's interests.

Samuelson (2003), who also has been critical of technologies that regulate through embedded code, believes that DRM systems may violate the fair-use provision of copyright law. For example, she notes that DRM technology allows content owners to exercise far more control over uses of copyrighted works in digital media than what is provided by conventional copyright law. The claim that DRM threatens fair use has also been echoed by Grodzinsky and Bottis (2007) who argue that this technology has not only become an obstacle to fair use but has also changed our conventional understanding of "private use as fair use." Like Elkin-Koren, Samuelson, and other critics, Grodzinsky and Bottis worry that DRM is designed to protect digital content in a way that enables private interests to define the parameters of copyright law. In this sense, DRM schemes have clearly tipped the balance in favor of copyright owners who can now determine how and by whom their content may be used.

9.2.2 DRM and the Music Industry

One controversial use of DRM in the music industry, which has alarmed many critics, gained public attention because of an incident involving Sony BMG Music Entertainment and its "rootkit" technology. What, exactly, are *rootkits*, and what purpose(s) do they serve? Doctorow (2014) defines rootkits as "programs that covertly modify a computer's operating system to blind it to certain files and processes."[5] The DRM-related rootkit controversy involving Sony is illustrated in the following scenario.

▶ **SCENARIO 9–2:** The Sony Rootkit Controversy

Sony BMG used a DRM system called Extended Copy Protection (XCP) to protect its music CDs. In 2005, a blogger named Mark Russinovich posted an article that described the characteristics of the software protection scheme used by Sony. In that article, Russinovich (2005) disclosed certain flaws in the design of Sony's software that manifested themselves as security holes that could be exploited by malicious software such as viruses or worms. He also noted that Sony provided no "uninstall" program to remove XCP. Sony responded to this criticism by releasing a "software removal utility."

But Russinovich, in a follow-up blog article, noted that Sony's removal utility had only exacerbated privacy and security concerns about the software. For example, he pointed out that the program merely "unmasked" the hidden files in the "rootkit" component of XCP, but did not actually remove the rootkit itself. In November 2005, Sony offered a "new and improved" removal tool to uninstall the rootkit from affected Microsoft Windows computers.

Some of Sony's critics accused Sony of violating the privacy of its customers by using code that created a "backdoor" into their customers' machines. Other critics also claimed that Sony's DRM program, which gave the company control over its customers' machines in the name of copyright protection, itself infringed copyright law. And some critics argued that Sony violated the open source license agreement (see Chapter 8) because of the way in which it used some open source software code to build its protection system. In late 2005, Sony decided to back out of its copy protection software, recalling unsold CDs from all stores and allowing customers to exchange their CDs for versions that did not include the controversial software.[6] ■

One DRM-related question that arises in connection with Sony's use of its controversial rootkit software is: Can users trust content owners (such as Sony BMG) who, via DRM-related tools, are easily able to (i) spy on them and (ii) control aspects of their computers and electronic devices? Another question that arises in this case is whether Sony's actions can be justified solely on the grounds that music (and entertainment) companies require DRM systems (like the one used by Sony BMG) to protect their intellectual property. But even if the answer to the latter question is "yes," we can still ask if that justifies a company's use of rootkits to surreptitiously track and spy on its customers.

Another area of tension involving the use of DRM by the music industry has to do with "interoperability" across the devices on which digital music can be played. Interoperability enables users to download and play music on a variety of digital devices. However, it also challenges the notion that downloadable content can and should be restricted to proprietary devices controlled by the company that owns an "online store," such as iPods in the iTunes store. Internationally, there have been some efforts to promote interoperability. For example, in 2006, France's National Assembly passed a law that would force distributors of online music in France to remove DRM so that music could be played on any device (Hesseldahl 2006). However, many owners and distributors of music content feared that removing DRM to support interoperability would also result in opening the door to file sharing of copyrighted material without compensation for the content owners and distributors.

In 2007, EMI announced that it would sell its music without DRM on Apple Inc.'s iTunes music store. One trade-off, however, was that non-DRM-formatted music would cost slightly more than DRM versions. Proponents of this change, including the late Steve Jobs, have suggested that if DRM restrictions were lifted on music, there might be an influx of new stores and players (Jobs 2007). The ongoing debate about which kinds of roles DRM will play in the contexts of online music and interoperability will likely continue.[7]

Our discussion of Internet regulation thus far has focused mainly on controversies associated with regulating *process* (i.e., in the commercial sector), as opposed to regulating content. As we will see, the latter type of regulation often becomes embroiled in thorny issues affecting free speech. We examine some of those concerns in Section 9.4. First, however, we consider a particular kind of challenge for Internet regulation that straddles the divide between process and content: e-mail spam.

▶ 9.3 E-MAIL SPAM

What is *spam*, and why is it problematic from a social and moral perspective? It is interesting to note that some defenders of spam see it as an activity protected by free speech. However, most Internet users see spam as something that is at best a nuisance and at worst a serious threat to the efficient and safe functioning of their computers and devices. Miller and Moor (2008) point out that according to some estimates, as much as 80% of e-mails sent could qualify as spam. But they also note that there are "dramatically different definitions" of what can count as spam.

9.3.1 Defining Spam

While there is no universally agreed-upon definition of spam, it is typically viewed as e-mail that is *unsolicited*, *commercial*, and sent in *bulk* to multiple users. Is this definition adequate? Because spam is *unsolicited*, it is also nonconsensual. However, not all nonconsensual e-mails are spam. If you have an e-mail account, you have probably received unsolicited e-mail messages requesting information from you or informing you about an upcoming event; they may have been sent to you because you are a member of a particular social networking service (SNS) or because you have an e-mail address associated with an academic institution, government organization, and so forth. You may have considered some of these messages annoying, but are they necessarily spam?

Another feature of our working definition of spam is that it is *commercial*. However, some commercial e-mail you receive can be in the form of advertisements that you have authorized a commercial Web site to e-mail you. For example, you could have registered on an e-mail distribution list for a department store at which you frequently shop, requesting to be informed

about upcoming sales and discount items. The e-mails you receive from this site, while commercial or promotional in nature, would not qualify as spam.

Spam is distributed in *bulk*, but not all e-mails distributed in that form necessarily qualify as spam. For example, some messages sent in bulk form (i.e., to an e-mail list) might have been directed at people in the group who are known by the sender; there could be some personal or professional connection between the sender and receiver of the e-mail message. So, our initial working definition of spam as e-mail that is "unsolicited, promotional, and sent in bulk" to multiple users would not seem adequate.

Miller and Moor believe that much of the popular discussion about spam in terms of what they describe as unsolicited commercial bulk e-mail (UCBE) is both "confused and degraded" because it fails to distinguish between UCBE that is "deceptive" and "intended to harm" and UCBE that is not. They also believe that the problems affecting e-mail spam can be better analyzed by focusing on a series of distinct, but interrelated, criteria such as the following:

- Content of the e-mail
- Intent of the sender
- Consequences of the receiver
- Consent of the receiver
- Relationship between the sender and the receiver
- Accountability of the sender and the degree of deception
- Number of identical e-mails sent[8]

Miller and Moor disagree with many critics of spam who tend to assume that all e-mail advertisements are deceptive. Alternatively, they believe that it is possible to distinguish between UCBE advertisements that (i) "misrepresent and are fraudulent" and (ii) "present information in a favorable light." They refer to the former as fraudulent UCBE (*F-UCBE*) and distinguish it from the nonfraudulent version they call nonfraudulent UCBE (*NF-UCBE*). They also believe that NF-UCBE requires a more complex ethical analysis than F-UCBE.

9.3.2 Why Is Spam Morally Objectionable?

Spinello (2006) believes that spam is morally objectionable for two reasons: one based on utilitarian grounds and the other on deontological considerations. In his view, spam not only has harmful consequences, but it also violates the individual autonomy of Internet users. First, consider some of the harmful consequences of spam—that is, its financial impacts, such as cost shifting and the consumption of valuable network resources. For example, spam consumes and strains valuable computing resources and thus contributes to the degradation of what Spinello calls the "fragile ecology of the Internet." Miller and Moor describe these kinds of abuses of the Internet as one more instance of "spoiling of the commons." (Recall our discussion of the "tragedy of the commons" in Chapter 8.)

Spinello argues that even if Internet resources were infinite and there were no negative utilitarian consequences, spam would still be morally objectionable because it does not respect individual users as persons. He believes that deontological arguments, such as Kant's (see Chapter 2), can be used to show why this is so. Recall that Kant argues that a practice has moral worth only if it can be universalizable. And, in Kant's system, a practice is universalizable only if it can coherently apply to all persons without exception. So, we need to ask: Could we universalize a coherent practice in which each e-mail user would allow spam to be sent and received by every other user? Could such a practice, if instituted, be logically coherent? On Kantian grounds, if spammers did not accept the principle that everyone should be able to send and receive spam, then they would be inconsistent. If spammers believed that only they

should be permitted to send spam, then they would be making an exception for themselves. And if they granted themselves this exception while relying on the good will of ordinary users not to engage in the practice of spamming others, then spammers would be treating ordinary users merely as a means to their ends. So, Spinello makes a plausible case for why spam can be considered morally objectionable on deontological as well as utilitarian grounds.

Miller and Moor believe that an adequate ethical analysis of spam also needs to take into consideration criteria such as accountability and deception—generally, the "more deceptive the content and the less accountable the sender, the more blameworthy the sender becomes." Employing their distinction between NF-UCBE and F-UCBE, they argue that F-UCBE should always be condemned, whereas some cases of NF-UCBE can be justifiable from a moral point of view. For example, they point out that a whistle-blower might send a message to a large commercial mailing list to alert recipients of an injustice or a danger. Here, the whistle-blower may have justifiable reasons for sending the e-mail broadly and for wishing to be anonymous. Miller and Moor believe that in this whistle-blowing scenario, the "intent" of the sender needs to be taken into consideration. So, there can be some cases where sending spam in the form of NF-UCBE would be justifiable.

It is one thing to say that spam, at least in its F-UCBE form, is morally objectionable, but it is another to ask what can be done about it from a legal and public policy perspective. Because spam is very similar to the "junk mail" that we receive via the postal delivery system, we might ask why the same laws that apply to physical junk mail do not also apply to electronic spam. Although there are similarities between the two forms of junk mail, there are also relevant differences; practical and financial constraints determine how much physical junk mail merchants can send, but the same kinds of constraints do not apply in the case of electronic spam.

Miller and Moor believe that e-mail spam is also analogous to unsolicited commercial phone calls. And they point out that the latter have been significantly reduced in the United States through legislation, even though they have not been altogether eliminated. But they also note that because of the "open" nature of Internet architectures and protocols, spam has been far more resistant to the kinds of legislative and technological solutions used to discourage unsolicited commercial phone calls.

Various state laws against spam have been enacted in the United States, and in 2003, the U.S. Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act. That law, which went into effect in 2004, specifies criminal penalties that include a fine of $250 for each spam e-mail. However, critics of the CAN-SPAM Act note that spammers who use ISPs outside the United States to send their spam e-mail cannot be prosecuted under this act, which cannot be enforced internationally. Some critics are also skeptical as to whether any kind of legislation, even international laws, can solve the problem of spam.

► 9.4 FREE SPEECH VS. CENSORSHIP AND CONTENT CONTROL IN CYBERSPACE

So far in this chapter, we have examined a set of regulatory issues that either involved, or had implications for, electronic commerce. We next turn our attention to regulatory issues involving the *content* of cyberspace. Such issues center on the question as to whether all forms of online speech should be tolerated. In some instances, regulatory concerns affecting online speech and online commerce overlap. For example, questions concerning spam, considered in the preceding section, straddle the divide; some purveyors of spam have defended their practice on the grounds of free speech. However, the issues we examine in the remainder of this chapter affect the regulation of Internet content and thus tend to fall mainly under the category of speech.

Note that in this and in the following sections, we do not address the censorship or suppression of "political speech" by nation-states—an issue that is hotly debated because of practices involving governmental regulation of the Internet in the People's Republic of China and other nondemocratic countries. That concern is however addressed in Chapter 10 in our examination of democracy and democratic ideals in cyberspace. In Section 9.6.1, we examine some tensions between free speech and censorship that arise mainly in the United States and in the European Union countries.

9.4.1 Protecting Free Speech

Do all forms of online speech in the United States deserve to be protected under the U.S. Constitution's guarantee of free speech? According to the First Amendment of the U.S. Constitution, "Congress shall make no law . . . abridging the freedom of speech, or of the press." This passage, consisting of merely 14 words, has often been quoted by libertarians who strongly believe that the government should not intrude in matters involving our constitutionally guaranteed right to free speech. We should note, however, that free speech is not an absolute right. As in the case of other rights contained in the Bill of Rights, which comprise the first ten amendments to the Constitution, the right to free speech is *conditional* in the sense that it is only a right if "all things are equal." While one's right to free speech protects his/her freedom to express controversial ideas concerning politics, religion, and so forth, it does not grant him/her the right to shout "Fire!" in a crowded shopping mall or a movie theater (an analogy frequently made by analysts describing the limits of free speech as a conditional right).

Also, during times of war, one's ability to speak freely is sometimes constrained. For example, in the period immediately following the attacks of September 11, 2001, some Americans labeled the news commentators, reporters, and talk show hosts who criticized the Bush White House as "unpatriotic." Ordinarily, such criticisms are considered normal and in accordance with the principle of free speech, which is presumed by political commentators and the press. But at other times, social norms and market forces rather than the law itself can regulate free speech. Television viewers who were offended by remarks they perceived as either anti-Bush or antigovernment pressured advertisers not to sponsor programs that expressed viewpoints that they believed were "unpatriotic." This, in turn, caused television networks either to cancel some programs or not to broadcast them in certain areas of the country. (Note that this is an example of Lessig's claim that, in certain cases, social norms and market forces can be more effective regulators than laws themselves.) Nonetheless, free speech is a broad right, cited time and again by publishers of unpopular tabloids and also appealed to by many who distribute pornography. Many believe, however, that some forms of speech on the Internet, including pornography, should be censored.

9.4.2 Defining Censorship

What, exactly, is censorship? Mathiesen (2008) characterizes censorship as limiting access to content by deterring either (i) the speaker from speaking or (ii) the hearer from receiving the speech. She also advances a more formal definition of censorship, claiming that to censor is to

> *restrict or limit access to an expression, portion of an expression, or category of expression, which has been made public by its author, based on the belief that it will be a bad thing if people access the content of that expression.*[9]

Catudal (2004) points out that an important distinction can be drawn between two types of censorship that he describes as "censorship by suppression" and "censorship by deterrence." Both forms presuppose that some "authorized person or group of persons" has judged some text or "type of text" objectionable on moral, political, or other grounds.

Censorship by suppression prohibits the objectionable text or material from being published, displayed, or circulated. Banning certain books from being published and prohibiting certain kinds of movies from being made are both examples of censorship by suppression. In this scheme, pornography and other objectionable forms of speech would not be allowed on the Internet.

Censorship by deterrence, on the contrary, is less drastic. It neither suppresses nor blocks out objectionable material, nor does it forbid such material from being published. Rather, it depends on threats of arrest, prosecution, conviction, and punishment of both those who make an objectionable text available and those who acquire it. Heavy fines and possible imprisonment can deter the publication and acquisition of objectionable content. Again, using Lessig's regulatory model, social norms, such as social disenfranchisement, personal disgrace, and public censure, can also work to deter individuals from engaging in the publication, display, and transmission of objectionable speech.

In the next two sections, we examine three key forms of "objectionable speech" in cyberspace: pornography, hate speech, and speech that can cause physical harm to others. In the following section, we focus on various forms of online pornography, including virtual child pornography, and we look at a series of laws that have been enacted to protect children and minors.

► 9.5 PORNOGRAPHY IN CYBERSPACE

Before examining the issue of pornography on the Internet, or what some call "cyberporn," it is instructive to understand what legally qualifies as pornography in general. It is often debated in terms of notions such as obscenity and indecent speech. In *Miller v. California* (1973), the court established a three-part guideline for determining whether something is obscene under the law and thus not protected by the First Amendment. According to these criteria, something is obscene if it

1. depicts sexual (or excretory) acts whose depiction is specifically prohibited by law;
2. depicts these acts in a patently offensive manner, appealing to prurient interest as judged by a reasonable person using community standards;
3. has no serious literary, artistic, social, political, or scientific value.[10]

These criteria have proved problematic in attempts to enforce pornography laws. For example, the second criterion includes three controversial notions: "prurient interest," "reasonable person," and "community standards." *Prurient* is usually defined as having to do with lust and lewd behavior, concepts that, in turn, have been challenged as being vague and arbitrary. Also, many ask who, exactly, counts as a "reasonable person." The notion of "community standard" would likely seem the most straightforward or least controversial of the three concepts—that is, until the advent of cybertechnology, when a community had been traditionally defined in terms of geographical space. But what, exactly, is a community in cyberspace? And when more than one community is involved in a dispute involving pornography, whose community standards should apply?

9.5.1 Interpreting "Community Standards" in Cyberspace

Interpretations of "community" and "community standards" were among the issues debated in a court case involving pornography and the Amateur Action (Electronic) Bulletin Board System. (Electronic bulletin board systems could be viewed as a type of online forum that functioned as a predecessor to contemporary Internet sites such as craigslist.) This bulletin

board system (BBS), which made sexually explicit images available to its members, was operated by a married couple who lived in California. Because it was an online forum, its contents were available not only to residents of California but also to users who had Internet access in other states (in the U.S.) and in other countries as well. A resident of Memphis, Tennessee, became a member of the BBS and then downloaded sexually explicit pictures onto his computer in Tennessee. Although including sexually explicit images on a BBS may not have been illegal in California, viewing such images was illegal under Tennessee state law. So, criminal charges were eventually brought against the operators of the BBS, who (though California residents) were prosecuted in Tennessee.[11]

The operators of this BBS were found guilty under Tennessee law of distributing obscenity, as defined under the local community standards that applied in Memphis. Not surprisingly, this case raised issues concerning what, exactly, was meant by "community standards" on the Internet. Can a community still be viewed or defined simply in terms of geography? Or, in an era of Internet-based social networking services (SNSs), such as Facebook and Twitter, should "community" be defined by other criteria? For example, can an online community be better understood as a computer-mediated forum where individuals who share common interests, regardless of geographical distance or proximity, come together? (We examine online communities in detail in Chapter 11.)

The Amateur Action case also raised another important issue affecting BBSs and online forums: Were the pornographic files actually *distributed* over the Internet by the operators of the BBS in California, as alleged? Or, instead, did the resident in Tennessee who downloaded them via the interstate telephone lines that transmit information between the two states *retrieve* those controversial files from the Internet? Questions involving both distribution and community standards in cyberspace contribute to the difficulty of interpreting and enforcing pornography laws online.

Many people first became aware of the amount of pornographic material available on the Internet through a news story entitled "CyberPorn," which appeared in *TIME* magazine in the summer of 1995. *TIME* reported that there were then 900,000 sexually explicit pornographic materials (pictures, film clips, etc.) available on the Internet. Many people, including most lawmakers, were outraged when they learned about the amount of pornographic materials that were so easily accessible to Internet users, including minors. Later, however, the *TIME* magazine story, based on an Internet study that had been conducted by a researcher at Carnegie Mellon University, was shown to be seriously flawed.

Although the Carnegie Mellon University study accurately reported the number of pornographic images and pornographic Web sites that were available, it failed to put this information into proper perspective—it made no mention of the fact that the percentage of pornographic sites relative to other sites on the Web was very low. However, the report caught the attention of many influential politicians, some of whom drafted legislation in response to what they saw as the growth of the "pornography industry" on the Internet. The result was the passage of the Communications Decency Act (CDA) in 1996.

9.5.2 Internet Pornography Laws and Protecting Children Online

The CDA caused controversy from the outset, especially the section referred to as the Exon Amendment, which dealt specifically with online pornography. The American Civil Liberties Union (ACLU) and other organizations challenged the constitutionality of CDA. A court in Philadelphia struck down CDA on grounds that it violated the U.S. Constitution; this court's ruling was upheld by the Supreme Court in 1997.[12] However, one section of the CDA, known as the Child Pornography Protection Act (CPPA) of 1996, was determined to be constitutional. According to CPPA, it was a crime to "knowingly send, receive, distribute, reproduce, sell, or possess more than three child pornographic images."[13] So even though CDA itself had been

struck down, supporters of that legislation were pleased that the section on child pornography still held.

In 1998, the U.S. Congress passed the Child Online Pornography Act (COPA). (We should note that COPA is sometimes confused with COPPA, the Children's Online Privacy Protection Act of 2000, which was designed to reduce the amount of information that could be collected from children under the age of 12 who use the Internet.) Many of COPA's proponents believed that this act would be upheld by the courts; but as in the case of CDA, COPA was ill-fated. In 1999, the U.S. Supreme Court ruled that COPA was unconstitutional.[14] The only remaining federal law in 1999 that was specifically directed at online pornography was the CPPA of 1996, a section of the original CDA. Although it appeared that CPPA would remain intact, many critics argued that provisions of this act also conflicted with the U.S. Constitution. In 2002, the Supreme Court, in a 6-3 ruling, struck down portions of CPPA as unconstitutional.[15]

In 2000, the U.S. Congress enacted into law the Children's Internet Protection Act (CIPA), designed to address concerns about children's access to "offensive content" over the Internet via school and library computers. CIPA was targeted specifically at schools and libraries, where federal and local governments have greater control. This law affects any schools or public libraries that receive federal funding in the form of "E-Rate" discounts (described in Chapter 10), which make certain technologies more affordable for eligible schools and libraries. According to CIPA requirements, schools and libraries would not receive the discounts offered by the E-Rate program unless they certified that they had an "Internet safety policy" in place. This policy also included technology-based protection measures to block or filter Internet access by minors to pictures that are considered (i) obscene, (ii) child pornographic, and (iii) harmful to minors.[16]

As in the case of CPPA and COPA, CIPA was eventually challenged in the courts. In 2001, several groups, including the American Library Association (ALA) and the ACLU, filed suit to prevent the enforcement of CIPA's filtering requirement in public libraries. In 2002, the U.S. District Court for the Eastern District of Pennsylvania ruled that the CIPA filtering mandate was unconstitutional. However, the District Court's decision was overturned by the U.S. Supreme Court, which upheld CIPA in a 6–3 decision in June 2003 (*United States v. American Library Assn. Inc.*, 2003).

Many legal analysts who closely followed the Supreme Court's ruling in CIPA suggested that no clear precedent had been established with respect to how online child pornography laws will be interpreted in the future. They believed that this was especially apparent in legal precedents for interpreting an appropriate scope of filtering in public libraries. (The Supreme Court's ruling in CIPA was a "plurality decision" because there was less than a clear majority in the justices' written opinions.[17]) Although CIPA provides protection for children in school and library settings, proponents of broad-based pornography legislation worried that CIPA fell short because it did not provide the kind of protection they believed children need outside those contexts. However, CIPA's critics argued that too much nonpornographic content was blocked in the process of protecting children.

Table 9-1 identifies the four online child pornography laws that have been enacted at the federal level (in the U.S.), and includes information about when the laws were passed and when three of them were eventually struck down.

9.5.3 Virtual Child Pornography

Critics have argued that online pornography laws, especially CPPA, broaden the definition of child pornography to include entire categories of images that many would not judge to be "child pornographic." Catudal (2004) notes that under CIPA, visual depictions of sexually explicit conduct that do not involve *actual* minors would still be included as child pornography. In fact, Catudal believes that the CPPA's definition of child pornography includes categories of images that some would judge "not pornographic at all."

TABLE 9-1 Internet-Specific Child Pornography Laws

CDA (Communications Decency Act)	Passed in January 1996 and declared unconstitutional in July 1996. The Supreme Court upheld the lower court's decision in 1997
CPPA (Child Pornography Protection Act)	Passed as part of the larger CDA, but not initially struck down in 1997 with the CDA. It was declared unconstitutional in April 2002
COPA (Child Online Pornography Act)	Passed in June 1998 and (portions) declared unconstitutional by the Supreme Court in February 1999
CIPA (Children's Internet Protection Act)	Passed in December 2000 and declared unconstitutional by a U.S. district court in 2002. The Supreme Court overturned the lower court's ruling in June 2003

Child pornography, according to CPPA, is "any depiction, including a photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct." The definition goes on to list four categories of such depictions:

A. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

B. such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct; or

C. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or

D. such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.[18]

Whereas category (A) images represent depictions of what has been traditionally regarded as child pornography, Catudal argues that the same is not true of category (B) images. For example, he considers the case of a 19-year-old girl who appears in a pornographic image in which she looks much younger. Sexual depictions of this sort are sometimes referred to as the "little girl" genre; they have been used in many artistic works. (The "little girl" type does not, by definition, actually involve little girls or minors of any age.) In the United States, the sexually explicit depiction of a "young-looking" 19-year-old would be considered child pornography under CPPA, but in some other countries, such as Norway, it would not. Catudal believes that CPPA fails to note that category (A) and category (B) depictions represent two different types of prurient images.

Note also that in categories (C) and (D), the pornographic image can consist of a depiction of someone who *appears* to be a minor engaging in sexual activity or a depiction that *conveys the impression* of a minor engaging in such an activity. So, a computer-generated image that does not refer to an actual human being would also qualify as a child pornography image under CPPA. In its decision to strike down portions of the CPPA, the Supreme Court reasoned that a distinction needed to be made between a pornographic image of an actual child and that of a "virtual," or computer-generated, image of a minor.

Some argue that because no real children are used in the production of virtual child pornography, no children are harmed in the process. However, Sandin (2004) argues that even if the production of virtual child pornography does not harm real children, it does not follow

that the *use* of virtual child pornography causes no harm to real children. Sandin suggests that a utilitarian argument could be made against allowing virtual child pornography if it is shown to have harmful consequences for real children. But Andrews (2010), who also makes an interesting case against virtual child pornography, worries that utilitarian arguments in and of themselves may not be sufficient to show that such behavior is unethical. So, Adams concludes that this issue should be tied to a

> much broader debate about the access of children to information of a sexual nature, without ignoring the differences between passive viewing of sexual activity (whether 'real' or 'virtual') and active virtual engagement.[19]

In our discussion of virtual reality (VR) in Chapter 11, we will see that "objectionable behavior" performed in virtual environments such as VR games, which portray only virtual or computer-generated images, can nonetheless cause real harm to real people. However, we will not continue with the debate about real vs. virtual harm here. Our purpose in this section has been to examine Internet pornography legislation that has been enacted to protect children online and to show why that legislation has been controversial, especially when it is extended to include virtual child pornographic images. We next consider how those laws apply in the case of "sexting."

9.5.4 *Sexting* and Its Implications for Current Child Pornography Laws

What is sexting, and what challenges does it pose for existing child pornography laws? Sexting is typically defined as the use of cell phones (or similar handheld electronic devices) to send nude or seminude photos of oneself to others. In some cases, these photos become widely distributed and can eventually end up on the Internet.

▶ **SCENARIO 9–3:** A Sexting Incident Involving Greensburg Salem High School

In 2009, six teenagers—three girls and three boys—at the Greensburg Salem High School in Pennsylvania were charged under child pornography laws in a sexting incident. The three girls, aged 14 and 15, who took nude or seminude photos of themselves on their cell phones and sent them to male classmates, faced charges involving the "manufacturing and dissemination of child pornography." The boys, who were aged 16 and 17, faced charges of possession of child pornography. (The nude pictures were discovered by Greensburg Salem High School officials when they seized a cell phone from a male student who was using it in violation of school policy.) The charges were later reduced to misdemeanors.[20] ■

Should the six teenagers have been charged with either dissemination or possession of child pornography? Were the original felony charges brought against them too harsh? Alternatively, are misdemeanor charges too lenient in cases such as this one? There does not yet seem to be any clear consensus on the answer to this question. Yet, the number of reported sexting incidents involving teenagers has increased sharply in recent years.

Next, consider two sexting incidents that each had very unfortunate outcomes—one resulting in the suicide of an 18-year-old female and one resulting in a felony charge brought against a male who had just turned 18. An Ohio resident—we will call her "Jill"—sent nude photos of herself via her cell phone to a boy, who then forwarded the pictures to others. The nude pictures of Jill were seen by some of her classmates at school as well as by others who lived in her community. As the photos became more widely distributed, Jill was taunted by some of her classmates as well as by others in her community. In May 2008, Jill took her life by hanging herself in her bedroom.[21]

A Florida resident, whom we will call "Phil," sent a nude picture of his ex-girlfriend to his friends and family, via his cell phone, following the couple's breakup. His ex-girlfriend was 16,

and Phil had recently turned 18 (the age at which one can be legally prosecuted as an adult in the U.S.). He was arrested by the police in Florida who charged Phil with sending child pornography, and he was later convicted of a felony offense. Consequently, Phil was required to register as a sex offender, which means that his name will appear on an Internet registry of sex offenders in Florida until he is 43. Phil was also expelled from college and was unable to find employment. Additionally, he is required to check with his probation officer if he plans to travel outside his home county (in the state of Florida).[22]

Can sexting crimes be understood and prosecuted in a manner that is consistent with our current legal framework? It would seem that sexting incidents have generated a "conceptual muddle" (Moor 2007), which needs to be resolved before we can frame coherent policies and laws to punish sexting offenses. Legal analysts point out that the current laws are inconsistent in their application from state to state. We have seen that states such as Pennsylvania and Florida have prosecuted, or have tried to prosecute, sexting cases as a felony offense. However, in other states, including Vermont, lawmakers have introduced legislation that would exclude teenagers who engage in sexting from being tried under child pornography laws and would instead make sexting a misdemeanor.[23] Advocates on both sides of this view, however, can agree on one thing: more consistent laws are needed.

Hilden (2013) believes that instead of applying older child pornography laws that were designed for "graver and much more exploitative contexts," we should "craft new laws designed specifically for sexting." She agrees with the critics of the Greensburg case, including the ACLU, who argue that the initial charges brought against the six Pennsylvania teenagers were "ill-grounded," because the child pornography laws under which the teenagers were first charged were intended to cover "lascivious displays of the genitals and/or sexual activity." Hilden believes that the teenagers involved in the Greensburg Salem High School incident were not guilty of this kind of behavior, especially since two of the girls were wearing bras and one was topless in the photos sent to the three boys. So, prosecuting the three girls under strict child pornography laws would be inappropriate.

Hilden also believes, however, that the prosecution of some teenagers under such laws would be appropriate in future cases of sexting that might involve "underage teens having sex, displaying their genitals in a lascivious way, or both." In these cases, she suggests that the behavior of the teenagers could validly "form the basis of child-pornography charges." Hilden also suggests that lawmakers should consider two kinds of exceptions to child pornography laws in sexting cases:

i. A "Romeo and Juliet" exception (which is sometimes used in statutory rape laws where consensus is involved)

ii. An "age-specific" exception

Hilden believes that the Romeo and Juliet exception could apply when the two parties to an act of sex are close in age (say, 18 and 16, or 15 and 17). She notes, for example, that a 16-year-old sexting a nude photo of herself or himself to someone roughly the same age is far less disturbing than a 16-year-old doing so at the invitation of a 40-year-old. Hilden asks us to imagine a 16-year-old, named Jane, who sends a nude photo of herself to her 18-year-old boyfriend, Bill. Here, Jane might be protected under the Romeo and Juliet exception (and thus be immune from prosecution).

But Hilden also points out that if Bill forwards the photo to one or more persons without Jane's consent, he should not be immune from prosecution. Hilden believes that while these exceptions do not provide a "bright line" in prosecuting sexting cases, they at least enable authorities to differentiate between a high school senior who takes and "sexts" a photo of a 13-year-old eighth grader, and is truly engaging in child pornography, and a sexting incident involving two teenagers in the same-age category. In this way, the exceptions would avoid the

need to impose severe criminal penalties on more or less same-age kids for what Hilden describes as "ugly immaturity," not crime.

One question that Hilden does not consider, however, is what would happen in the case where a teenage girl sends an uninvited nude photo of herself to an older man. In this case, would the man receiving the unsolicited photo be liable for prosecution under child pornography laws merely for having (or having had at some point) the nude photo of the teenager on his cell phone or electronic device? An actual case involving sexting between a 52-year-old man and a 14-year-old female occurred in Georgia in 2009. In this incident, the older man was trying to set up a "sexual rendezvous" with the young female. The girl sent him nude photos that she had taken of herself on her cell phone. Here, of course, the controversies raised go well beyond sexting—for example, they also include questions of intended child molestation or pedophilia.[24]

It would be interesting to consider what would happen if this 52-year-old man had made no sexual advances toward the 14-year-old girl and still received the pictures? It is not clear whether he still could be criminally charged with possessing child pornography on his cell phone. So, it would seem that answers to questions of this type would also need to be spelled out more clearly and explicitly in any future legislation drafted for sexting that incorporates "age-specific exceptions."

What can we conclude about sexting as it relates to our examination of child pornography in this section? We can agree with critics that most teenagers who have been prosecuted so far for sexting have not engaged in behavior that meets the threshold of crimes intended for prosecution as felonies under child pornography laws. Yet, sexting is a serious offense and thus needs to be dealt with appropriately in the legal and judicial systems. In the meantime, it seems that enacting some kind of federal legislation with standards that could be applied to sexting cases occurring in all states would be the best short-term solution.

▶ 9.6 HATE SPEECH AND SPEECH THAT CAN CAUSE PHYSICAL HARM TO OTHERS

In addition to pornography, which is sometimes viewed as "obscene" speech, hate speech and forms of speech that can cause physical harm to individuals and communities have both caused controversy in online contexts. We briefly examine some controversies affecting each.

9.6.1 Hate Speech on the Web

Hate speech on the Internet often targets racial and ethnic groups. For example, white supremacist organizations such as the Ku Klux Klan (KKK) can include offensive remarks about African Americans and Jews on their Web pages. (Recall our brief discussion of the KKK in Scenario 9–1.) Because of the Internet, international hate groups, such as "skin heads" in America, Europe, and Russia, can spread their messages of hate in ways that were not previously possible. Whereas much of the focus in the United States has been on controversial Internet speech issues that involve online pornography, European countries such as France and Germany have been more concerned about online hate speech. For example, Germany's Information and Communications Act was designed to censor neo-Nazi propaganda. But the law applies only to people who live in Germany; it cannot regulate the speech transmitted by ISPs outside that country. Girasa (2002) believes that if the German government had tried to enforce this law, countries such as the United States would likely have refused to extradite individuals to Germany.

In France, it is illegal to sell anything that incites hate and racism. However, Nazi and KKK memorabilia are auctioned daily on Web sites such as Yahoo that have an international reach.

In 2000, a French judge ruled that Yahoo must "make it impossible" for people in France to access sites selling that kind of material. Yahoo complied, and as a result, Nazi-related items are no longer available on Yahoo's French site (www.yahoo.fr). But French citizens who use an ISP outside France could potentially access the sites that are banned in France.[25]

In the United States, some "hate-watch" Web sites, such as the Southern Poverty Law Center (SPLC) "Intelligence Project" (http://www.splcenter.org), monitor online hate speech aimed at racial minorities. In an effort to counter the effectiveness of "hate sites," these hate-watch Web sites have exposed the existence of various hate organizations to the public. The SPLC site also features a Hatewatch blog and it includes a detailed map with physical locations of various hate groups, which it identifies under categories such as KKK, neo-Nazi, racist skinhead, and so forth. Ironically, perhaps, the information available on these sites also provides an easy way for consumers of hate speech to locate and visit particular hate sites that serve their interests. (In Chapter 10, we examine some of these concerns from the vantage point of race and cybertechnology, as opposed to the perspective of online hate speech.)

Numerous Web sites have promoted white supremacist hate speech. One such site was operated by James von Brunn who fatally shot an African American museum guard at the Holocaust Museum in Washington, DC, in 2009. On his site (holywesternempire.com), von Brunn included hate speech aimed at Jews and African Americans. (In fact, his site was included on the SPLC's list of notorious hate sites.) A few days before von Brunn shot his victim, he transferred control of his Web site to Steve Reimink who described the 88-year-old von Brunn as a "sick individual." But Reimink's message also included "code," familiar to many white supremacists, suggesting that Reimink's remarks were not sincere.[26]

Some antiabortion groups in the United States have set up Web sites dedicated to distributing (hate-related) information about doctors who perform abortions. These sites have also included information about where these doctors live, what times they travel to and from abortion clinics, where they go in their free time, etc. As in the case of the white supremacist rhetoric used by radical groups in the United States, this type of speech can also result in physical harm to others. Some information made available on antiabortion Web sites has been linked to the murder of doctors who perform abortions. In 2009, for example, Dr. George Tiller, who performed late-term abortions in Kansas, was murdered by an antiabortionist. Information about Tiller was available to Tiller's murderer via a Web site set up by an antiabortionist group (http://www.dr-tiller.com/), which described Tiller as "America's most notorious abortionist" and as "Tiller the Killer." This site also included information about Tiller's employees and assistant abortionists.

9.6.2 Online "Speech" that Can Cause Physical Harm to Others

Some forms of hate speech on the Internet are such that they might also result in physical harm being caused to individuals (as in the case of the antiabortionist sites described earlier). Other forms of this speech, however, are by the very nature of their content, biased toward violence and physical harm to others. Consider two examples of how speech communicated on the Internet can result in serious physical harm: one involving information on how to construct bombs and another that provides information on how to abduct children for the purpose of molesting them. Should this information be censored in cyberspace? Information of this kind was available before the Internet era and it may even have been (and still may be) available in some libraries. If it is available elsewhere, should it be censored on the Internet?

Critics point out that Internet access now makes it much easier to acquire all kinds of information, including information about how to make and do things that cause physical harm. They also note that it is possible to access and read this information in the privacy and comfort of one's home. Even more disturbing is that it is now far easier for international and domestic

terrorists to obtain information about how to construct bombs. So, some believe that these are good enough reasons for censoring this kind of speech on the Internet.

Recall our discussion in Section 9.1.1 about whether the Internet should be conceived as a broadcast medium, like television or radio, or as a place, like a bookstore. We saw that the rules that apply in each are significantly different. Viewing the Internet as a medium of some sort makes it far easier to control the dissemination (or broadcast) of certain kinds of information than viewing it as a public place, such as a bookstore or library. If the Internet is viewed in the latter sense, however, it is more difficult to ban controversial forms of speech such as hate speech and speech that can cause physical harm to others. So, the debate continues about which kinds of speech, if any, should be regulated on the Internet.

▶ 9.7 "NETWORK NEUTRALITY" AND THE FUTURE OF INTERNET REGULATION

So far in this chapter, we have analyzed a wide range of controversies affecting cyberspace regulation. While some concerns have focused on issues involving the regulation of commerce, others have centered mainly on issues that affect speech (or content) in cyberspace. All of these regulatory concerns, however, have been examined within the context of a "neutral" Internet. We conclude this chapter by examining the controversial debate involving *network neutrality*, and we consider what kinds of implications the outcome of this debate will likely have for regulating and accessing the Internet in the future.

9.7.1 Defining Network Neutrality

What, exactly, is network neutrality, or "net neutrality," as it has commonly come to be called? Tim Wu, an Internet policy expert at Columbia University, describes it as a principle in which "a maximally useful public information network aspires to treat all content, sites, and platforms equally."[27] In explaining the key elements underpinning the net neutrality principle, Wu draws an interesting analogy between a neutral Internet and other kinds of networks, which he claims are also implicitly built on a "neutrality theory." Using the example of the neutral nature of the electric grid, he notes that the same grid that "worked for the radios of the 1930s" also works for the "flat screen TVs of the 2000s." Wu also notes that the electric grid doesn't care whether you plug in a computer, an iron, or a toaster; thus, it is the grid's "general purpose and neutral nature" that make it extremely useful, as well as a "model of a neutral, innovation-driving network."[28]

Will the Internet, like the electric grid, remain a neutral network? The principle of net neutrality has been at the center of a contentious debate between two groups: *neutrality opponents*, which include major U.S. telecommunication companies as well as some conservative law makers, and *neutrality proponents*, consisting of a wide coalition comprising numerous organizations that are commercial and noncommercial, liberal and conservative, and public and private. Proponents also include many consumer groups and ordinary users, as well as the founders of the Internet (Lessig and McChesney 2006).

Proponents argue that the Internet had been conceived of and implemented as a neutral network from the outset, even if no regulatory laws or formal policies had been in place to enforce it. However, this basic principle has been questioned and challenged in recent years by neutrality opponents. The tension that had been brewing between the two groups came to the fore in the U.S. in 2005, when the FCC officially adopted four broad neutrality principles in an effort to (i) "deregulate the Internet services provided by telephone companies" and (ii) "give consumers the right to use the content, applications, services and devices of their choice when using the Internet."[29]

In 2008, one service provider, Comcast, was accused of deliberately slowing down access to (and effectively blocking users from) a popular P2P file-sharing site. That year, the FCC filed a formal complaint against Comcast for its actions; although it did not fine the service provider, the FCC did require that Comcast cease blocking the P2P site in question. Next, Comcast challenged the FCC's position in court, and in 2010 a federal appeals court ruled in Comcast's favor.

Following the appeals court's decision, the FCC approved a policy that some viewed as a "compromise" position, which effectively created two classes of Internet access: one for "fixedline providers" and one for the "wireless net." Some critics saw this compromise as a policy of "net semineutrality." While that FCC policy officially banned fixed line broadband providers' services from both "outright blocking" and "unreasonable discrimination" of Web sites or applications, it also arguably provided more "wiggle room" to wireless providers such as Verizon and AT&T.[30]

9.7.2 Some Arguments Advanced by Net Neutrality's Proponents and Opponents

Proponents of net neutrality tend to argue that America's largest telecommunications companies, including AT&T, Comcast, Time Warner, and Verizon, want to be "Internet gatekeepers" who can:

- guarantee speedy delivery of their data via "express lanes" for their own content and services, or for large corporations that can afford to pay steep fees;
- slow down services to some sites, or block content offered by their competitors;
- discriminate "in favor of their own search engines, Internet phone services and streaming video."[31]

Net neutrality's opponents tend to respond to these charges by claiming that the telecommunications companies have no plans to block content or services, slow down or "degrade" network performance for some sites, or discriminate against any users. Instead, they argue that these companies simply want to stimulate competition on the Internet and that doing this will result in increased:

- Internet speed, reach, and availability for users (in the United States)
- Economic growth, job creation, global competitiveness, and consumer welfare[32]

However, many critics remain skeptical about the neutrality opponents' real intentions, and some point to an incident in 2008 (mentioned earlier) in which Comcast intentionally degraded network performance by slowing down access to a popular file-sharing site.

9.7.3 Future Implications for the Net Neutrality Debate

Lessig and McChesney (2006) argue that one important benefit of net neutrality in the past has been that it has served to minimize control by the network owners. So, many neutrality proponents worry about the future of the Internet in the absence of a net neutrality principle. In general, proponents believe that the consequences of an Internet without a neutrality principle would be devastating for at least three reasons:

1. access to information would be restricted, and innovation would be stifled;
2. competition would be limited because consumer choice and the free market would be sacrificed to the interests of a few corporations;
3. the Internet will look more like cable TV, where network owners will decide which channels, content, and applications are available (and consumers will have to choose from their menus).[33]

However, the opponents of net neutrality—especially large telephone and cable companies in the United States—see the matter very differently. For one thing, broadband providers claim that since 2008 they have invested more than $250 billion dollars to expand Internet access to broadband technology to homes and businesses in the United States. For another, they claim that broadband industry is now responsible for supporting more than six million American jobs.[34]

Neutrality opponents have continued to press hard for policies that would grant the telecommunication companies more flexibility and control. In January 2014, the FCC proposed a regulatory policy that some neutrality proponents believed would protect key aspects of net neutrality. However, this policy was also challenged in the courts and was rejected by a federal court on the grounds that the FCC was trying to regulate Internet providers as if they were the same as public utilities. (The latter are typically more heavily regulated than "information services" providers.) However, net neutrality supporters were encouraged that the federal court, in its 2014 ruling, upheld and confirmed the FCC's authority to regulate broadband on the Internet.[35]

In early 2015, the FCC deliberated over a new policy that would reclassify broadband as "telecommunications services," similar to traditional telephone service; this move would also enable Internet broadband to be regulated more heavily. Additionally, it would give the FCC more authority in regulating business mergers and agreements between content companies like Netflix and (service) providers like Comcast. Under the FCC's enforcement, Comcast and other Internet providers would be also banned from entering into so-called "paid prioritization" agreements with content providers.[36]

On February 26, 2015, the FCC officially adopted its new policy. According to Fernholz (2015), this policy can be summarized as requiring ISPs to follow three principles: (i) no blocking of legal content; (ii) no "throttling," or deliberately slowing down the delivery of data; and (iii) no paid prioritization, where ISPs could set up "fast lanes" for some content providers but not for others. Baum (2015) believes that ordinary Internet users will benefit from the policy because they will not be "relegated to a second class information highway," while ISPs may be adversely affected because they may now feel pressure to "invest more resources on building additional bandwidth." And because building more bandwidth is very expensive and would likely result in less profit for ISPs, those companies may elect not to make that investment.[37]

Some believe that the net neutrality dispute is far from settled and that it is still not yet clear which direction the U.S. government will ultimately take on it in the long term. But if, as some fear, the Internet eventually becomes a multitiered entity with respect to access, that is, where some parties (e.g., those who either control content or can afford to pay for premium access) are privileged or favored at the expense of ordinary users, the future Internet may become a "discriminatory medium." Concerns about discriminatory online access may also raise some new, or at least exacerbate some existing, equity and access-related issues affecting the "digital divide"—a topic that we examine in detail in Chapter 10.

▶ 9.8 CHAPTER SUMMARY

In this chapter, we have considered some challenges to regulating cyberspace. Specifically, we considered Internet regulation issues from two different perspectives: the regulation of commercial activities on the Internet and the regulation of content in cyberspace. We saw that decisions to view cyberspace as a medium rather than as a public place or space, or vice versa, are significant, because they determine which kinds of rules apply to regulating speech on the Internet. We also saw that the enactment of formal or explicit laws is only one way to regulate cyberspace. As Lessig and others have noted, much regulation of the Internet is being accomplished through technology itself, especially (software) "code." Future regulatory decisions will determine whether the Internet remains "neutral," or open, or whether it evolves into a different kind of entity.

Unfortunately, not all Internet regulation controversies were able to be examined in the limited space of this chapter. For example, one concern not considered here has to do with online defamation and who should be legally liable for defamatory remarks made in a particular online forum. (To date, many online defamation-related questions are still not resolved.) Another controversy not examined in this chapter involves the question of who should be responsible for regulating online "classifieds services" such as craigslist.com and backpage.com, especially with regard to ads affecting "adult services." While craigslist.com has taken a self-regulatory kind of approach by eliminating these kinds of services from its site, backpage.com has since been accused of facilitating sex trafficking and child exploitation by listing various adult services on its site. Yet, as of August 2015, there does not seem to be any clear regulatory body in place to monitor the kinds of sites that engage in these services. So, it would seem that some significant policy vacuums still need to be filled regarding Internet regulation.

▶ REVIEW QUESTIONS

1. In discussing "cyberspace regulation," why is it useful to distinguish the question "Can cyberspace be regulated?" from the question "Should cyberspace be regulated?"
2. Describe the arguments for why cyberspace should be viewed as a medium, and why it should be viewed as a "place."
3. How does the way we interpret cyberspace—that is, as a "place" or as a medium—affect the kinds of policies that can be used to regulate it?
4. What are the two different senses of "regulation" we examined, and how can they be applied to the regulatory issues involving cyberspace?
5. Identify the four modalities that Lawrence Lessig believes can be used to regulate behavior, and give an example of how each can be applied to regulating behavior on the Internet.
6. What does Lessig mean by the following claim: "In cyberspace, code is the law"?
7. What is digital rights management (DRM) technology, and why is it controversial?
8. Why does Cory Doctorow believe that the DMCA (Digital Millennium Copyright Act) works hand in hand with DRM technology to control the flow of digital information?
9. What does Niva Elkin-Koren mean when she asserts that information policy is becoming increasingly "privatized"? Why does she believe this is a problem?
10. What is e-mail spam, and why is it controversial?
11. What is the CAN-SPAM Act? Is it effective in deterring spam? Explain.
12. How does Kay Mathiesen define censorship? Describe the criteria that Jacques Catadul uses to distinguish between "censorship by suppression" and "censorship by deterrence."
13. What is pornography? Why is interpreting what is meant by "community standards" especially difficult in establishing pornography laws for cyberspace?
14. Describe the three Internet-specific child pornography laws that were passed in the 1990s but later struck down by the U.S. Supreme Court.
15. How is the Child Internet Pornography Act (CIPA) of 2000 both similar to and different from earlier laws affecting child pornography online?
16. What is "virtual child pornography," and why is it controversial?
17. What do we mean by "hate speech"? Give some examples of hate speech in cyberspace.
18. What is meant by "speech that can cause physical harm to others"?
19. What is network neutrality (or "net neutrality"), and why is it controversial?
20. Describe some of the arguments advanced by "neutrality proponents" and by "neutrality opponents." Which position do you find more convincing?

▶ DISCUSSION QUESTIONS

1. Have DRM systems gone too far, as some critics claim? Recall the 2005 Sony BMG copy protection case involving the controversial "rootkit" problem (examined in Scenario 9-2). Should Sony have been allowed to use a DRM system that cannot easily be uninstalled when circumstances warrant it? Do companies like Sony need strong DRM systems to ensure the protection of their intellectual property rights? What kind of compromise position might be reached between users and content owners in the ongoing debate about DRM systems?
2. Assess the (consequence-based and duty-based) arguments that Richard Spinello uses to show that e-mail