PART 4

Regulatory, Compliance and Liability Issues

CHAPTER 11

Government Regulation

It is true that Congress gave the [Federal Communications] Commission broad and adaptable jurisdiction so that it can keep pace with rapidly evolving communications technologies. It is also true that the Internet is such a technology, indeed, arguably the most important innovation in communications in a generation. Yet notwithstanding the difficult regulatory problem of rapid technological change posed by the communications industry, the allowance of wide latitude in the exercise of delegated powers is not the equivalent of untrammeled freedom to regulate [Internet] activities over which the statute fails to confer ... Commission authority.[1]

LEARNING OUTCOMES

After you have read this chapter, you should be able to:

- **Identify several ways antitrust laws have been applied to online activities.**
- **Discuss how far into the online world the U.S. government's broad power to tax has extended, and provide examples.**
- **Explain the requirements for a state to obtain tax jurisdiction over an out-of-state business operating online.**
- **Identify in what ways governments have sought to regulate content, including user-generated content.**
- **Discuss how market regulation and consumer privacy rights intersect.**

Introduction

Computer software, many cyberspace programs and functions, and other so-called information goods are considered by many to be public goods, that is, goods that are both **nonrival** and **nonexcludable**. For example, when music is exchanged on the Internet by way of an MP3 file or a YouTube video, its exchange does not limit others' use (i.e., nonrival), and the consumption of these files is often difficult to restrict (i.e., nonexcludable). Digital technologies are easy to reproduce and distribute, and copying them is difficult to control. So, cyber-technologies are public goods, right? Not so fast. The inventors, producers, and distributors of some information goods argue that such goods

[1] *Comcast Corp. v. FCC,* 600 F.3d 642, 661 (D.C. Cir. 2010) (internal quotation marks and citations omitted).

are not—or should not be—public goods, but private goods. Private actors should reap the benefits of the goods they have produced. If they do not, the incentive to produce goods voluntarily is reduced. If information goods are made available for free, no one will be willing to pay for them.

Into this political game—or, some say, political vacuum—step governmental regulators. Now, no one gets a free ride. The government might tax the provision of the good or might provide the public good by way of an unfunded mandate. Advocates of regulation argue that it is necessary to protect consumers from a monopoly's unfair advantage. But others contend that the Internet began as open and borderless and should remain so; every act of regulation creates borders and takes away some of that openness.

The question whether government—or the marketplace, or another force—should regulate the Internet is part of the broader debate about Internet governance.

> *Today, it appears that the different approaches being taken to Internet governance at the national, regional and international levels may limit, or even threaten, the long-term viability of the Internet as a global communications and information medium. The World Summit on the Information Society appeared to recognize the seriousness of these conflicts, by deciding to launch a process for examining Internet governance comprehensively at the global level, within a UN framework. In light of these developments, it is possible to conclude that the future history of global Internet governance may not be all that different from the past history of telecommunications and ICT (internet communications technology) governance — i.e. that there is a need to harmonize governance approaches on a global basis, in order to reap the potential benefits of Internet technology.*[2]

This chapter looks at the various ways the United States and other governments regulate activity on the Internet and in other online media, including enacting and enforcing antitrust laws, taxation, regulation of content, and protection of consumers by way of laws and regulations. These issues will be discussed in the context of the broader debate as to who governs the Internet, and how it is governed.

The Need for Regulation

In the United States, there is a strong history of self-regulation, the theory being that the markets should be largely free to regulate themselves. This has been the case particularly for Internet regulation. When this technology first emerged, regulators were concerned about over-regulating for fear that too much regulation would stymie the growth of its economic potential.

At times, market self-regulation fails and regulators need to step in. This, too, has been the case with respect to the Internet. In recognition of increasing concerns that the web was becoming a kind of lawless "Wild, Wild West," but cognizant of the negative consequences of over-regulation, U.S. lawmakers began to focus on regulation in some of the most critical areas. For example, as a result of the economic impact of **cybersquatting**, lawmakers enacted the Anticybersquatting Consumer Protection Act. Also, after incidents demonstrated the vulnerability of children's privacy online, Congress enacted the Children's Online Privacy Protection Act. Overall, what has emerged is a hybrid system of regulation in which new Internet-specific laws and regulations,

[2]Don MacLean, "Herding Scrödinger's Cat's: Some Conceptual Tools for Thinking about Internet Governance: Background Paper for the ITU Workshop on Internet Governance, Geneva, 26–27 February 2004," n.1 (email: donjmac@sympatico.ca).

pre-Internet laws and regulations, and market self-regulation each play a role in regulating Internet conduct.

Ways to Regulate Behavior

Given that it is necessary to regulate behavior online, the next question is how that will be best accomplished. There are four main ways to regulate behavior: (1) through laws; (2) by the markets; (3) via funding sources; and (4) by means of technology. As will be discussed further below, each of these has a role to play in the online realm.

Law One of the leading ways to regulate behavior is through law, and law is significant force in the regulation of online behavior. The Internet is regulated by a mix of new laws enacted to address specific concerns unique to online activities and old laws that have been interpreted to apply online. Although laws are necessary to the regulation of the Internet, laws alone cannot ensure effective regulation. The Internet and related technologies change very rapidly, and laws often move very slowly.

Markets Markets also play an important role in the regulation of behavior. Pricing and other business terms often determine who consumers are and how much of something they purchase. The market has been particularly important in regulating the Internet. As discussed, initially regulators had a largely hands-off approach with respect to the regulation of the Internet, the theory being that over-regulation would have a negative impact on the growth of ecommerce and other online activity. Into this relative legal vacuum moved industry self-regulation.

Markets continue to be a major factor in the present-day regulation of the Internet, particularly in the area of privacy. Despite concerns about privacy online, in the United States, Internet privacy remains lightly regulated under law and market pressures serve as a regulating force. For example, when companies experience privacy breaches or commit violations of trust, their customers might cease using their services and take up with a competitor that can offer better privacy protection. The backlash that resulted when Facebook made changes to its privacy controls is one example of the market regulating conduct. Although regulators and a number of U.S. senators took issue with Facebook's changes,[3] arguably the bigger impact in Facebook's policies came from user backlash, which eventually resulted in changes to the site's privacy options.[4]

Funding Sources The availability of funding can also contribute to the regulation of online activity. When investors stand behind certain business models and business practices, the development of those activities is encouraged. Conversely, business models and business practices that are unable to draw in investment are likely to die away.

Technology The final significant factor that can regulate online behavior is technology. While opening up new opportunities for unauthorized online activity, technology can also help to regulate conduct online and ensure that Internet users are acting in compliance with their obligations under law and contract. For example, music services such as iTunes place technological controls on their music files that effectively limit the ability of users to use the files. In this way, the technology regulates users' conduct and helps to ensure that users comply with their license agreements and applicable law.

---

[3]Jared Keller, "The Facebook Privacy Wars Heat Up," *The Atlantic*, May 6, 2010, available at: http://www.theatlantic.com/science/archive/2010/05/the-facebook-privacy-wars-heat-up/56344/.

[4]CNN Tech, "Facebook, Facing Criticism, Ramps Up Privacy Options" (May 26, 2010), http://articles.cnn.com/2010-05-26/tech/facebook.privacy_1_new-privacy-controls-privacy-settings-facebook-users?_s=PM:TECH.

Regulation of Markets

Governments are concerned with concentrations of economic power that distort optimum market conditions are distorted—a sort of free, unregulated marketplace. This marketplace has many sellers and many buyers who freely enter into transactions with full knowledge of the terms and the bargained-for goods or services. **Antitrust** laws regulate and encourage competition.

Overview of U.S. Antitrust Law

United States antitrust law is the body of laws that prohibits anticompetitive behavior and related unfair business practices. At the core of antitrust law is prohibition of any monopoly that restrains competition, using its size to unfairly compete. Antitrust laws seek to allow competition in the marketplace, targeting activities that lessen or discourage competition. Regulators generally look at whether a company is erecting a barrier of entry into a market for other companies. Outside of the United States, antitrust law is known simply as competition law.

The two main U.S. antitrust laws are the **Sherman Act** and the **Clayton Act**. The Sherman Antitrust Act, 15 U.S.C. Sections 1–7, limits cartels and monopolies, empowering the federal government to investigate and prosecute companies and organizations that violate the Act. Its purpose is to oppose the combination of entities that might harm competition.

Section 1 of the Sherman Act states, "Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal." Thus, in prosecutions for violating the Act, the government is required to prove (1) that an agreement has been reached (2) that unreasonably restrains competition and (3) that affects interstate commerce.

Section 2 states, "Every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce among the several States, or with foreign nations, shall be deemed guilty of a felony…." Thus, proof of a violation of Section 2 of the Sherman Act requires a showing of (1) monopoly power in a particular market and (2) willful acquisition or maintenance of that power.

The Clayton Antitrust Act of 1914, 15 U.S.C. Sections 12–27 and 29 U.S.C. Sections 52–53, supplements the Sherman Act and focuses on prevention of anticompetitive practices. There are four sections of the Clayton Act.

- One section prohibits **price discrimination** between different purchasers of the same product, when the discrimination substantially lessens competition or creates or furthers a monopoly.
- Another part prohibits sales conditioned on (1) a purchaser agreeing not to deal with the seller's competitors or (2) the purchaser also buying a different product at the same time (tying), if one of these acts substantially lessen competition.
- Another section prohibit any merger or acquisition that substantially lessens competition.
- There is a section that prohibits an individual from being a director or corporate officer of competing corporations (**interlocking directorates**).

In the United States, the Federal Trade Commission (FTC) through its Bureau of Competition and Bureau of Economics, and the Department of Justice (DOJ) via its Antitrust Division, enforce the federal antitrust laws. Additionally, state attorneys general enforce state and federal antitrust statutes, and private persons "injured" in their "business or property" by an antitrust law violation may file civil suits against alleged violators. In an antitrust case like the cases discussed below, the plaintiff is usually the government. The defendant is a business or an organization.

Google

Interlocking Directorates

In 2009, Section 8 of the Clayton Act, which prohibits so-called interlocking directorates, made headlines when Google's CEO resigned from Apple's board of directors following the FTC's investigation into a possible Section 8 violation. Shortly thereafter, another individual resigned from the boards of both Apple and Google, and then a third person, a director at Google, resigned from the board of Amazon amid the FTC's investigation into the Google-Amazon relationship. Although such overlapping roles are not uncommon, the FTC warned that "coopetition"—marketing and developing products or services in one market while competing in another—poses the risk of improper agreements and information-sharing that could hurt consumers, running afoul of U.S. antitrust laws.

Monopolization in Restraint of Trade

Another aspect of the Clayton Act was triggered in 2009 when Google, which in addition to its other services has the second-most-successful mobile advertisement network, proposed to purchase the leading mobile ad network, AdMob, for a proposed $750 million. After the FTC launched an investigation, Apple acquired Quattro Wireless (the third largest mobile ad network) in a separate transaction. The FTC then closed its investigation of the Google-AdMob deal without taking adverse action against Google. Although the FTC asserted that the proposed acquisition "necessitated close scrutiny because the transaction appeared likely to lead to a substantial lessening of competition in violation of Section 7 of the Clayton Act," it cited "important developments in the mobile advertising marketplace" such as Apple's acquisition of Quattro "that should mitigate the [potential] anticompetitive effects of Google's AdMob Acquisition."[5]

Some criticized the FTC's conclusion, arguing that Google's purchase of AdMob would directly violate the Clayton Act's prohibition on mergers or acquisitions that substantially lessen competition. It would eliminate Google's direct, largest, and only real competitor. It would create a concentration in the market—75 percent—around double what the FTC usually allows; whenever a market share concentration in a highly concentrated market reaches 30–40 percent, the FTC usually objects. Critics pointed to the extraordinarily high price Google would pay for AdMob as evidence that Google was acquiring market power and argued that the deal would effectively foreclose competition in the market, harming consumers, advertisers, developers, smart-phone manufacturers, publishers, and broadband providers. In other words, a Google-AdMob deal would create the classic type of situation sought to be prevented by antitrust law.

Tying

Another aspect of antitrust law with frequent application to the online realm is **tying**. When a seller requires the buyer to purchase a second product or service in conjunction with the purchase of the buyer's choice, and the tying substantially affects competition, the antitrust laws are triggered.

Apple has allegedly run afoul of antitying laws on several occasions. In 2009, Apple told software developers making applications for Apple's iPhone, iPod Touch, and iPad,

[5]Federal Trade Commission, *Statement of the Commission Concerning Google/AdMob*, FTC File No. 101-0031 (May 21, 2010).

that they had to use Apple programming tools. This was reminiscent of Apple's position in litigation in 2008, right after it introduced the iPhone, when Apple sought to contractually bind consumers to use only Apple applications on their iPhones and only a particular carrier—AT&T Mobility—for their phone service.[6]

IN RE APPLE & AT&TM ANTITRUST LITIGATION
596 F. Supp. 2d 1288 (N.D. Cal. 2008)

FACTS

This litigation arose from Apple, manufacturer of cellular telephone equipment, joining with AT&T Mobility (AT&TM), supplier of voice and data services, to provide to consumers a cell phone with service. Pursuant to an arrangement between the companies, the purchaser of an Apple iPhone became bound contractually to use ATTM as its cell phone service provider.

> *Plaintiffs allege that consumers were offered iPhones only if they signed a two-year service agreement with AT&T Mobility. Plaintiffs allege, however, that unknown to consumers, the companies had agreed to technologically restrict voice and data service in the aftermarket for continued voice and data services, i.e., after the initial two-year service period expired.*[7]

In the proceedings on Apple's motion to dismiss, Apple contended that the plaintiffs did not state a claim under § 2 of the Sherman Act. Apple argued that the plaintiffs alleged neither legally cognizable markets under the Sherman Act, nor legally sufficient monopolization of those markets.

JUDICIAL OPINION (DISTRICT COURT JUDGE WARE)

Denying Defendants' Motion to Dismiss, the court determined that Plaintiffs stated a cause of action upon which relief could be granted.

> *Section 2 of the Sherman Act prohibits monopolization, attempted monopolization and conspiracy to monopolize "any part of the trade or commerce among the several States." 15 U.S.C. § 2. To state a valid claim under the Sherman Act, a plaintiff "must allege that the defendant has market power within a 'relevant market.'"* Newcal Industries, Inc. v. IKON Office Solution, *513 F.3d 1038, 1044 (9th Cir. 2008) (citing* Eastman Kodak Co. v. Image Technical Services, Inc., *504 U.S. 451, 481, 112 S. Ct. 2072, 119 L. Ed. 2d 265 (1992)).*[8]

Thus, the two factors that must be proven are (1) a legally cognizable market and (2) monopolization of that market.

In *In re Apple*, the district court looked at the plaintiffs' market allegations relating to two markets: (1) an aftermarket in voice and data services for the iPhone, and (2) an aftermarket in iPhone applications. Apple contended there was no relevant aftermarket for the iPhone voice and data services. But the plaintiffs alleged that although they agreed to the two-year plan, they "did not agree to use ATTM for five years," yet "Apple and ATTM enforced this exclusivity by programming and installing software locks on each iPhone to prevent purchasers from later switching to another wireless carrier," which bound consumers for five years and prevented them switching carriers, even if they paid a $175 termination fee to ATTM.[9] The court found that these allegations recited facts that, when presumed to be true, supported the existence of an aftermarket for iPhone voice and data services under the *Newcal* standard.

> *Principally, Plaintiffs have alleged an aftermarket for iPhone voice and data services that "would not*

(*Continued*)

[6]See Mark DeFeo, *Unlocking the iPhone: How Antitrust Law Can Save Consumers From the Inadequacies of Copyright Law*, 49 B.C. L. Rev. 1037 (2009).

[7]596 F. Supp. 2d at 1294.

[8]*Id.* at 1301.

[9]*Id.* at 1303.

exist without" the primary market for iPhones, and is thus "wholly derivative from and dependant on the primary market." Newcal*, 513 F.3d at 1049. Plaintiffs' Complaint is also adequate to the extent the alleged aftermarket is predicated on an initial contractual relationship between Defendants and iPhone purchasers.* Id.[10]

Further, the plaintiffs alleged a present injury, even if they had not yet tried to switch their voice and data service.

Plaintiffs are alleging that at the point of purchase and initiation of service, Defendants involuntarily impose on consumers a contract exclusivity restriction which restricts their freedom from that point forward for at least the next five years and conceivably for the life of the iPhone … The fact that some consumers might not have sought to switch service and thus do not realize the restriction which the Apple/ATTM Agreement has imposed on them does not alter the effect of Plaintiffs' allegation that their freedom in the aftermarket has already been taken from them.[11]

Likewise, the plaintiffs sufficiently alleged an aftermarket for iPhone applications. Not only did Apple create iPhone-specific applications, it also built technological restrictions into the phone and policed those restrictions. This was sufficient to state a claim under § 2 of the Sherman Act.[12]

Having found that these two markets existed, the court then concluded that Apple possessed power in the relevant markets—a key factor to a finding of monopolization.

Plaintiffs have alleged that Defendants "achieve[d] market power through contractual provisions that they obtain[ed] in the initial market" for iPhones and attendant two-year service contracts. Through the initial iPhone purchase and contracting, Defendants are alleged to have gained the "special access" to consumers by which they are then able to lock purchasers into use of ATTM … [and] into use of only applications in which Apple maintained a financial interest. Apple is then alleged to have enforced its special position through technological controls.…[13]

Accordingly, the court denied Apple's motion to dismiss the plaintiffs' antitrust claims relating to both the iPhone voice and data services and iPhone applications aftermarkets.

CASE QUESTIONS

1. On what basis did the district court reject Apple's argument that the plaintiffs' claims should be dismissed because they had not actually suffered any injury?
2. ***Ethical Consideration:*** Suppose your company's engineers figured out how to manufacture applications that worked on the iPhone or another Apple product. Should you manufacture and sell them, so you can share in some of Apple's success? Would such a move find support in antitrust law? On the other hand, is it possible without running afoul of antitrust laws for a competitor make a similar product?
3. Suppose a customer purchases several Apple devices, downloads Apple-compatible applications, and puts her personal data on the devices. Apple then makes it impossible for this consumer to use her own data on another device of her choice. Should regulators step in? Why or why not? Are consumers really harmed if various services are bundled together, but everything is free?

Maintaining a competitive marketplace thus is one of the U.S. government's primary areas of regulatory interest. While the Sherman Act and the Clayton Act were created long before the information age, their relevance to the computer industry, especially software goods and online services, is apparent. As the *In re Apple* case and Google-AdMob deal illustrate, companies that provide information goods and services must operate within the parameters of existing antitrust regulations. Federal enforcers will prosecute

[10] *Id.*

[11] *Id.* at 1304.

[12] *Id.*

[13] *Id.* at 1305, 1306.

statutory violations, and they will scrutinize—and possibly prevent—proposed actions that threaten to lessen competition.

Net Neutrality

Another area of federal regulation with importance to the online world, and related to competition, is the question of the extent to which governments and **Internet Service Providers (ISPs)** may restrict Internet sites, platforms, and equipment. **Net neutrality** is a principle that all movement and content on the Internet should receive equal treatment. Proponents of net neutrality—usually users, content providers, small online businesses, and some large businesses—argue that a *neutral* Internet encourages innovation and they argue against telecommunications providers' restriction of bandwidth for certain Internet services. They oppose broadband providers blocking Internet content and applications of competitors, adhering to the principle that users paying for the same level of service should receive the same level of service. The net-neutrality argument is another aspect of the larger question about the scope of competition regulation in cyberlaw in the 21st Century.

As a very general matter, the Internet is content-neutral. ISPs do not, for the most part, block, slow down, or speed up the transmission of data based on what it is, who sent it, or who will receive it.

There are opponents to the concept of complete net neutrality, among them those who argue that some regulation is necessary. Some ISPs, other members of the telecommunications industries (especially cable companies), and large hardware companies have argued that some data discrimination, such as packet filtering of viruses, is positive and even necessary to a functional Internet. They insist that more regulation by the Federal Communications Commission (FCC) would actually discourage innovation by preventing ISPs from charging higher fees for tiered services. And they point out that some applications, such as those that convey life-saving telemedicine or facilitate emergency services, are deserving of higher priority.

The FCC oversees the issue of net neutrality because ISPs are considered information services, akin to public utilities. In 2005, the FCC adopted the following Policy Statement with regard to the neutrality of the Internet:

> *[T]o ensure that broadband networks are widely deployed, open, affordable, and accessible to all consumers, the Commission adopts the following principles:*
>
> - *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to access the lawful Internet content of their choice.
> - *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.
> - *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet,* consumers are entitled to connect their choice of legal devices that do not harm the network.
> - *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to competition among network providers, application and service providers, and content providers.[14]

[14]Federal Communications Commission, Policy Statement, FCC 05-151 (Sept. 23, 2005).

Google

Google owns around 65 percent of the search engine market. Google's competitors—Microsoft, Yahoo, and AT&T among them—argue that antitrust implications arise when Google's search engine directs users to Google services. Google's position has been that it is not a monopoly and that linking to its own services benefits consumers.

The same argument was made in *Comcast v. FCC*.

COMCAST CORP. v. FEDERAL COMMUNICATIONS COMMISSION
600 F.3d 642 (D.C. Cir. 2010)

In a 2010 decision, the District of Columbia Court of Appeals held that the Federal Communications Commission (FCC) did not have the legal authority to regulate the way Internet service providers (ISPs) manage user traffic. That is, the FCC did not currently have the authority to enforce net neutrality.

FACTS

In 2007, some of the subscribers to Comcast's high-speed Internet service found out that Comcast was interfering with their use of applications for peer-to-peer networking. These peer-to-peer programs, which allow users to directly share large files with one another, consume large amounts of bandwidth.

Two nonprofit advocacy organizations filed a complaint with the FCC. They sought a declaratory ruling that Comcast's actions violated the FCC's Internet Policy Statement entitling consumers to access "the lawful Internet content of their choice," and "to run applications and use services of their choice." Comcast's response was that it had to interfere with peer-to-peer programs in order to manage scarce network capacity.

After the FCC decided that Comcast had "significantly impeded consumers' ability to access the content and use the applications of their choice," and that Comcast's method of bandwidth management "contravene[d] … federal policy," because there were other "options it could use to manage network traffic without discriminating" against peer-to-peer communications, Comcast challenged the FCC's authority to impose net neutrality obligations on broadband providers such as Comcast. Comcast protested that the FCC was trying to officially set net neutrality regulations and that it did not have the jurisdiction to do so.[15]

JUDICIAL OPINION (CIRCUIT JUDGE TATEL)

The court held that the FCC lacks the authority to require broadband providers to give equal treatment to all Internet traffic flowing over their networks.

> *Acknowledging that it has no express statutory authority over [an Internet service provider's network management] practices, the Commission relies on section 4(i) of the Communications Act of 1934, which authorizes the Commission to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions." 47 U.S.C. § 154(i). The Commission may exercise this "ancillary" authority only if it demonstrates that its action—here barring Comcast from interfering with its customers' use of peer-to-peer networking applications—is "reasonably ancillary to the … effective performance of its statutorily mandated responsibilities." The Commission has failed to make that showing.*[16]

The court set out the two-part standard for determining when the FCC may properly exercise its so-called ancillary jurisdiction: "'only when two conditions are satisfied: (1) the Commission's general jurisdictional grant under Title I [of the Communications Act] covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities.'"[17] The court then reiterated the rule

(*Continued*)

[15]600 F.3d at 644-45.
[16]*Id.* at 644 (citation omitted).
[17]*Id.* at 646 (citing *Am. Library Ass'n v. FCC*, 406 F.3d 689, 691-92 (D.C. Cir. 2005).

that "[t]he Commission's exercise of ancillary authority over Comcast's network management practices must, to repeat, 'be independently justified.'"[18]

The *Comcast* court ultimately rejected the FCC's argument that it had jurisdiction over Comcast based on congressional policy statements. In earlier cases, such policy statements supported an exercise of ancillary jurisdiction because there was also an express delegation of authority; here, there was no such authority. Reining in the FCC, the court said that were it to accept the FCC's arguments, the FCC would have no reason "to stop there"—there were few regulations applicable to common carrier services, broadcast services, or cable services that the FCC "would be unable to impose upon Internet service providers."[19]

It vacated the FCC's order:

> *It is true that "Congress gave the [Commission] broad and adaptable jurisdiction so that it can keep pace with rapidly evolving communications technologies." Resp't's Br. 19. It is also true that "[t]he Internet is such a technology,"* id.*, indeed, "arguably the most important innovation in communications in a generation,"* id. *at 30. Yet notwithstanding the "difficult regulatory problem of rapid technological change" posed by the communications industry, "the allowance of wide latitude in the exercise of delegated powers is not the equivalent of untrammeled freedom to regulate activities over which the statute fails to confer … Commission authority."* NARUC II*, 533 F.2d at 618 (internal quotation marks and footnote omitted).*[20]

CASE QUESTIONS

1. What must be shown for the FCC to exercise its ancillary authority?
2. Has the FCC's statutory authority kept pace with evolving technology? Why or why not? Does the dominance of the Internet call for more or less FCC regulation?
3. ***Ethical Consideration:*** Should consumers be allowed to use as much bandwidth as they want, knowing that they can get around this particular regulatory trap? Do companies that share large files, using large amounts of bandwidth, owe any responsibility to their ISPs? To other Internet users?

The period between 2005 and 2010 was seen as a time of increasing action by the FCC in enforcing its net neutrality policies, but, as the *Comcast* decision showed, the extent of its authority has been challenged. As the stakeholders continue to debate the complicated issue of net neutrality in the United States, it is worth noting that in the United States the Internet is quite open and unregulated as compared to governmental regulation of ISPs in some countries such as China and Russia.

In the absense of governmental regualtion on the issue, private companies are beginning to take a leading role in attempting to regulate net neutrality. In August 2010, Google and Verizon jointed together to issue a proposal for regulation that contrasts with prior FCC proposals on net neutrality. Their proposal is based upon the concept of equal treatment of most Internet traffic. It would, however, exempt cellular networks and yet-to-be-developed broadband services from the restrictions.[21] More specifically, the Google and Verizon proposal would:

- Discourage online providers from slowing or favoring certain traffic on the wired Internet;
- Allow the creation of new networks that provide faster delivery of content or services for a fee;

[18] *Id.* at 651 (citation omitted).

[19] *Id.* at 655.

[20] *Id.* at 661.

[21] Amy Schatz and Amir Efrati, "Verizon, Google Map Traffic Plan The Two Say Proposal Eases 'Net Neutrality' Debate; Critics Say It Could Create Private Networks," WSJ.com, Aug 10, 2010, available at: http://online.wsj.com/article/SB10001424052748704388504575419542307824622.html?mod=WSJ_hpp_LEFTWhatsNewsCollection#ixzz0xBNyqmuC.

- Keep cellular-based Web services largely unregulated; and
- Limit the FCC's authority over broadband Internet lines.

This proposal is a prime example of how private companies are endeavoring to fill voids left by the absence of governmental regulation.

Wireless Spectrum Management

Management of the **wireless spectrum** is another area in which the FCC places a key role. One hears similar arguments as those made in the net neutrality debate when studying the question of the extent to which the federal government should manage the wireless spectrum. On the one hand are those who urge centralized governmental ownership and regulation of the wireless spectrum; on the other are those who advocate for a hands-off approach.

Electromagnetic waves move through space at different frequencies, which together make up the electromagnetic spectrum. The radio frequency (RF) spectrum is the part of the electromagnetic spectrum for radio frequencies. The range of frequencies from 3kHz to 300 kHz can be used for wireless communication.

In most countries, the RF spectrum is the property of the state. The main purpose of managing the RF spectrum is to maximize the amount of available RF, optimizing its use and, conversely, to minimize radio spectrum "pollution" (i.e., interference). Other spectrum management goals include designing allocations for short- and long-range frequencies, coordinating wireless communications with others, and advancing the invention and introduction of new wireless technologies.

Among United Nations nation-states, the International Telecommunications Union (ITU) manages the use of the RF spectrum. The ITU is divided into three sectors, including the Radiocommunication Sector, which decides the operational procedures and technical characteristics for wireless services and performs other spectrum management functions; the Telecommunication Standardization Sector, which develops technical and operating standards; and the Telecommunication Development Sector, which works to expand the telecommunications infrastructure in developing nations.

In the United States, the FCC regulates domestic nonfederal spectrum use, and the National Telecommunications and Information Administration (NTIA) manages the spectrum for the federal government. Like other regulators, the FCC and NTIA use the so-called "command-and-control" approach to spectrum management in which the regulator is a centralized authority. Because the command-and-control approach initiated with early wireless communications, when interference was more of an issue such that each band needed to be dedicated to a single provider, some argue that such an exclusive approach is outmoded and no longer necessary.

Those who support the command-and-control model argue that some beneficial communication services would not be profitable enough to attract private providers, that such services are enforced by way of license agreements, and that the there is an advantage to standardization, especially in networked industries. Critics of this approach contend that RF spectrum management should be cooperative. It should balance stakeholder interests through user education and regulatory enforcement. Regulations should address politics, economics, physics, and practical reality. The argument is that RF spectrum management in the United States especially is outdated and unnecessarily complex in some areas but too permissive in others.

Spectrum scarcity has emerged as a major issue for those trying to initiate new wireless services, yet studies have shown that there is unused spectrum available. This artificial

limitation to accessing parts of the RF spectrum arguably could be remedied by changes to the current approach to spectrum management.

Two suggested approaches are the *spectrum commons* and the *spectrum property rights* models. Under the spectrum commons approach, the spectrum is like a physical commons, to which the people have certain access rights, although no one owns the commons as property. Under the spectrum property rights approach, portions of the spectrum may be privately owned, and allocation of parts of the spectrum is dictated by market forces. Most famously, economist Ronald Coase advocated for ownership of parts of the spectrum as the most efficient use of the spectrum. Advocates argue that such an approach would promote innovation efficiency. Critics argue that individual spectrum owners could hold up parts of the spectrum for high compensation in return for its use.

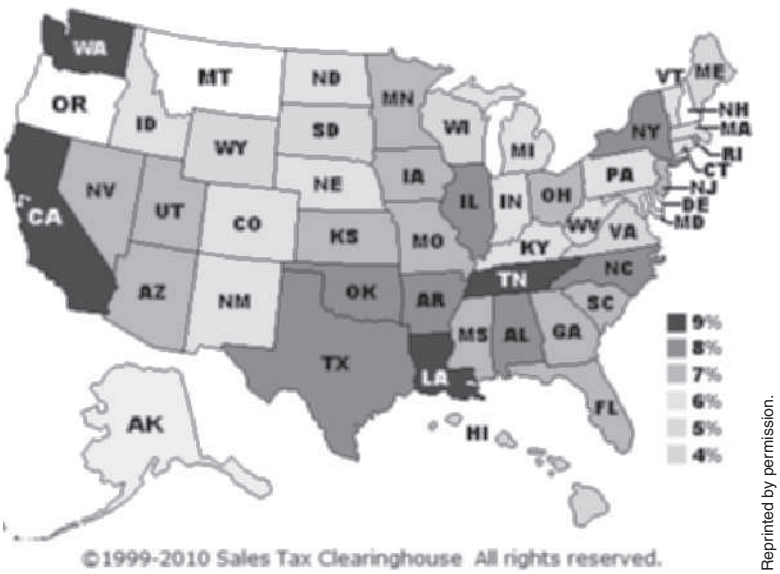
Regulation of Fiscal Policy

Fiscal policy is another significant area of regulation. There are a number of public policy goals with respect to taxation. The first consideration is neutrality, i.e., the system for taxation should be both platform neutral and content neutral. The second goal is efficiency, i.e., the system should be simple to administer and should involve minimal compliance costs. In short, it should have the largest coverage at the lowest rate.

Many states do not collect taxes on online transactions. As many consumers move their shopping to the online realm, such states are losing enormous revenue. A recent study estimated 2008 uncollected **sales tax** revenues from online sales at about $3.9 billion. This loss of tax revenue by the states has sparked debate in Congress and in state and local governments as to whether taxes should be imposed on online transactions, as well as who should standardize online taxing.

These debates have gained strength as the global financial crisis has left many states in a financially precarious position. Sales tax rates range considerable from state to state, as demonstrated in Exhibit 11.1. With rates going up to nearly 9 percent in certain states,

EXHIBIT 11.1 Sales Tax Rates for the United States



Reprinted by permission.

the loss of revenues attributed to uncollected taxes on ecommerce transaction is a very palpable loss for many states. As discussed further herein, a number of states are considering new ecommerce sales taxes.

The ability of states to impose sales tax on ecommerce transactions is not without limits. The Due Process Clause and the Commerce Clause of the U.S. Constitution regulate the extent to which states may impose sales tax. From a constitutional perspective, there are a number of requirements that must be met for a tax to be valid. The tax must be fairly related to the services provided by the state. The tax cannot discriminate. The tax must be fairly apportioned, and the business at issue must have a substantial nexus with the taxing state.

Problems with ecommerce taxation arise due to the fact that sales taxes are generally imposed based upon the physical presence of a business, while online services and products are generally sold from remote locations. The out-of-state ebusiness must have a **nexus** or physical connection with the taxing state in which the customer is located before it is obliged to collect and remit sales tax to the state taxation authorities. The physical presence requirement usually takes the form of a retail store, warehouse, employees, or sale representatives doing business in the taxing state. The taxing state must prove this nexus before an out-of-state company is required to collect tax from the buyer and remit it to the state. States may not require online companies to collect and remit sales taxes from their customers when those companies do not have a physical presence in the state.

In *Quill v. North Dakota*,[22] the U.S. Supreme Court held that the Commerce Clause of the U.S. Constitution requires an out-of state merchant to have a physical presence in a state before it can be obligated to collect its taxes.

QUILL CORP. v. NORTH DAKOTA
504 U.S. 298 (1992)

FACTS

Plaintiff in this case, the state of North Dakota, filed an action in state court to require Quill Corporation (Quill), an out-of-state mail order house, to collect and pay a use tax on goods purchased for use in the state. The trial court determined that a seller whose only connection with the customers in the state was by common carrier or the mail lacked the requisite minimum contacts with the state. The state supreme court reversed, holding that the Commerce and Due Process Clauses did not any longer require a physical presence in the state in order for the state to exercise its power over a company. Despite the fact that Quill, a Delaware corporation, had no employees living or working in North Dakota, the court held that advancements in technology and the mail order business as a whole rendered obsolete the law that required a physical presence in the state.

JUDICIAL OPINION (JUSTICE STEVENS)

The Supreme Court of the United States described North Dakota's tax in the following way:

> *North Dakota imposes a use tax upon property purchased for storage, use, or consumption within the State. North Dakota requires every "retailer maintaining a place of business in" the State to collect the tax from the consumer and remit it to the State.*[23]

The state included in the meaning of a retailer, a person who engages in regular or in systematic solicitation of a consumer market in North Dakota. The Supreme Court analyzed the Due Process Clause and the Commerce Clause separately in evaluating the state supreme court's decision.

(*Continued*)

[22]504 U.S. 298 (1992).

[23]*Id.* at 302 (citing statute).

"The Due Process Clause 'requires some definite link, some minimum connection, between a state and the person, property or transaction it seeks to tax.'"[24] This standard has been construed in the past to mean that any company that purposefully avails itself of the benefits of an economic market is considered to have a minimum contact with the state. As long as the tax is related to that benefit, the tax would be proper under the Due Process Clause.

The Commerce Clause, observed the Court,

> *expressly authorizes Congress to "regulate Commerce with foreign Nations, and among the several States." It says nothing about the protection of interstate commerce in the absence of any action by Congress. Nevertheless, … the Commerce Clause is more than an affirmative grant of power; it has a negative sweep as well. The Clause … "by its own force" prohibits certain state actions that interfere with interstate commerce.*[25]

One of the instances in which the Commerce Clause would prohibit state actions would be when the state taxes someone who does not have a substantial nexus with the taxing state. The state supreme court reasoned that when one has minimum contacts with the state, the substantial nexus test for Commerce Clause purposes would also be fulfilled. But the U.S. Supreme Court ruled that it is possible to have minimum contacts for purposes of the Due Process Clause, and still not have a substantial nexus for purposes of the Commerce Clause. The history of the Commerce Clause dictates that in order to have a substantial nexus with a state, one must have a physical presence there.

CASE QUESTIONS

1. Based on the standards articulated in the case summary, should the state be allowed to impose a use tax on Quill even though it does not have a physical presence in the state?
2. Is this the right decision? Should a state be able to impose income taxes on a company whether or not it has a physical presence, as the state supreme court held? Or, was the U.S. Supreme Court correct?
3. ***Ethical Consideration:*** Is this decision fair? Does the decision have the effect of withholding taxes from states that really rightfully deserve them? Quill was doing business in North Dakota—shouldn't Quill ethically be obligated to pay taxes to a state that generated it so much revenue?

Although the *Quill* decision explicitly allowed Congress to enact legislation for the states to impose sales and use taxes on products sold by an out-of-state merchant, to date it has failed to do so. This has not, however, stopped states from attempting to collect sales tax for ecommerce transactions from retailers based outside of the state. Businesses often resist and many cases have resulted. Exhibit 11.2 summarizes the positions commonly taken by the parties in these cases.

Many states technically require local residents to pay so-called **use tax** on such purchases, but most taxpayers ignore those rules. This concept may become clearer in context. Imagine you wish to purchase a new book. You have a couple of options for doing so. First, you can go to your local bookstore and purchase the book, in which case you

EXHIBIT 11.2 Summary of Positions in Tax Cases

PARTY	POSITION
Plaintiff (always a state)	Plaintiff asserts the Defendant business has a sufficient presence in the state to justify imposition of the tax collection burden; because the business takes advantage of the benefits of doing business in this state, it must pay its way.
Defendant (always a business)	Defendant asserts that the state taxation law violates the Constitution because the federal government regulates interstate commerce and the state tax is unduly burdensome to interstate commerce. In the alternative, the business's contacts with the state are not sufficient to justify imposition of the tax collection burden.

[24] *Id.* at 306 (citation omitted).

[25] *Id.* at 309 (citations omitted).

will be charged sales tax on your purchase. Alternatively, you can make your purchase at an online retailer, in which case (unless you reside in one of a handful of states), you will not be required to pay sales tax on your purchase.

Given that we are in the Internet age, when state (and even national) boundaries are increasingly less significant, it is not too surprising that the concept of "physical presence" has given rise to a number of interesting disputes. In reviewing the cases, consider how judicial decisions are accomplishing the same goal as ecommerce sales tax legislation would. As the appellate court noted in the *Borders* case, courts "face with increasing frequency issues at the junction of Internet technology and constitutional principles."[26]

BORDERS ONLINE, LLC. v. STATE BD. OF EQUALIZATION
129 Cal. App. 4th 1179, 29 Cal. Rptr. 3d 176 (2005)

FACTS

Borders Group Inc. (Borders) owns many stores in California as well as an online website, Borders Online, LLC (Online). One of the policies that the company has in place is that purchases made through Online can be returned in one of the many Borders stores throughout California. The policy specifically stated that

> *"You may return items purchased at Borders.Com to any Borders Books and Music store within 30 days of the date the item was shipped. All returns must be accompanied by a valid packing slip (your online receipt and shipping notification are not valid substitutes for a packing slip on returns to stores). Gift items may be returned or exchanged if they are accompanied by a valid gift packing slip. You may not return opened music or video items, unless they are defective."*[27]

Because of this relationship, the tax board determined that Borders was Online's representative, operating in the state for the purpose of selling Online's goods. Therefore, Online was considered to be making income in California and was required to pay a use tax. The tax board found that Online was covered by Cal. Rev. & Tax Code § 6203(c)(2) because (1) Borders was Online's authorized representative in California for the purpose of accepting returns from Online's California customers, and (2) the taking of returns constituted "selling" for purposes of the statute. In so ruling, the board concluded that "selling" includes "all activities that are an integral part of making sales." The board reasoned that Online's favorable return policy was designed to induce potential customers who might otherwise not make an online purchase to place orders, and thus the policy was "integral" to selling in ecommerce transactions. The Board also ruled that Online had a sufficient physical presence in California (through Borders) to satisfy the Commerce Clause of the United States Constitution.

The trial court agreed and granted summary judgment in favor of the Board. Online appealed to the California Court of Appeal.

JUDICIAL OPINION (JUDGE RIVERA)

The court concluded that Online was subject to California's use tax.

> *A use tax on interstate sales is "a tax on the privilege of use of property by the buyer" who purchases goods that would not otherwise be subject to a sales tax. California imposes a use tax "on the storage, use, or other consumption in this state of tangible personal property purchased from any retailer … for storage, use, or other consumption in this state…." The tax is paid by the purchaser but is collected by the retailer. A retailer that fails to collect the appropriate use taxes becomes indebted to the state for the amount owed. … The question, then, is whether Online had a "representative" or "agent" in California acting "under the authority of" Online for the purpose of "selling" personal property.*[28]

On this point, the court determined that Borders acted under Online's authority and was its agent.

(*Continued*)

[26] *Borders Online, LLC v. State Bd. of Equalization,* 129 Cal. App. 4th 1179, 1184, 29 Cal. Rptr. 3d 176, 178 (2005).

[27] 129 Cal. App. 4th at 1185-86, 29 Cal. Rptr. 3d at 179.

[28] *Id.*, 129 Cal. App. 4th at 1188, 1189, 29 Cal. Rptr. 3d at 181-82.

The trial court found that Online's return policy posted on its website provided "undisputed evidence" "confirm[ing] that Borders was [Online's] authorized agent or representative for the purpose of accepting returns of Online merchandise from California purchasers." It held this finding was supported by the fact that (1) each Borders store in the state would accept returns and provide a refund, store credit or exchange of Online's merchandise; (2) Borders encouraged its store employees to refer customers to Online's web site; and (3) receipts at Borders stores sometimes invited patrons to "Visit us online at www.Borders.com." The trial court concluded, "Borders' practice of providing unique and preferential services to Online purchasers by offering cash refunds to any purchaser of Online merchandise who wanted one, when it could refuse to do so for customers of Online's competitors, indicates that Borders provided such preferential services because it was Online's authorized agent or representative."

…[T]here is no dispute either that Online announced on its website that Borders was authorized to accept Online's merchandise for return, or that Borders would provide customers with an exchange, store credit, or a credit card credit. By accepting Online's merchandise for return, Borders acted on behalf of Online as its agent or representative in California.

… Online claims it had no "control" over Borders's action but does not dispute that Borders implemented the return policy posted on Online's website. Online also notes there was no written agreement between Online and Borders, but "[t]he creation of an agency relationship is not dependent upon the existence of a written agreement." In fact, "[t]he relationship may be implied based on conduct and circumstances, as well as by ratification." It therefore does not matter, as Online claims, that Borders did not have the subjective belief it was Online's agent. By accepting Online's merchandise under the terms of Online's return policy, Borders was effectuating Online's policy, even if it was also Borders's own policy. The undisputed facts show Borders acted as Online's agent or representative and therefore Online meets the first part of section 6203(c)(2)'s definition of "'[r]etailer engaged in business in this state,'" as a "retailer having [a] representative [or] agent … operating in this state ...."[29]

The court also held that Borders was "selling" for the purpose of the applicable statute.

The trial court concluded that by providing refunds and exchanges to Online's customers pursuant to Online's return policy, Borders was engaged in "selling" as that term is used in section 6203(c)(2). The court reasoned that "the term 'selling' may properly be defined to include all activities that constitute an integral part of inducing sales. Such a definition fairly captures the common understanding of this term."

The term "selling" is not defined in the statute. The Board construed the term to include "all activities that are an integral part of making sales," and concluded that this interpretation accords with its "common usage." The Board reasoned, "When out-of-state retailers that make offers of sale to potential customers in California authorize in-state representatives to take returns, these retailers acknowledge that the taking of returns is an integral part of their selling efforts. Such an acknowledgement comports with common sense because the provision of convenient and trustworthy return procedures can be crucial to an out-of-state retailer's ability to make sales.

… We think the Board's interpretation of the term "selling" is persuasive. The Board appears to have thoroughly considered the meaning of the term, and its reasoning that the act of "selling" encompasses offering other inducements to purchase is consistent with at least one later pronouncement. In contrast, Online's narrow interpretation would mean that even if a local representative were to provide dramatic incentives to California customers to purchase the out-of-state retailer's goods, no tax could be imposed unless the representative is actually involved in the solicitation of the sale or the sale transaction itself.[30]

Finally, the court also determined that the lower court's ruling was consistent with the Commerce Clause.

(*Continued*)

[29] *Id*, 129 Cal. App. 4th at 1189, 1191, 29 Cal. Rptr. 3d at 182, 183–184 (citations omitted).

[30] *Id*., 129 Cal. App. 4th at 1192-93, 29 Cal. Rptr. 3d at 185 (citations omitted).

… A tax passes constitutional muster only if it is applied to "'an activity with a substantial nexus with the taxing State.'"… The question is whether … the activities performed by Borders on its behalf were "'significantly associated with [Online's] ability to establish and maintain'"

…We have already determined that Online's return policy was part of its strategy to build a market in California. We further note that Borders's efforts on Online's behalf were not limited to accepting returns from-and providing exchanges and credit card refunds to-Online customers. Borders's receipts were sometimes imprinted with "Visit us online at www.Borders.com," and Borders's employees were encouraged to refer customers to Online to find merchandise not available at Borders stores. The cross-selling synergy was also maintained by the use of similar logos, by the link to Borders' webite from Online's website, and by the sharing of some market and financial data between the two entities. Online generated more than $1.5 million in sales in California in 18 months. These facts amply support the conclusion that Online had a representative with a physical presence in the State and the representative's activities were "'significantly associated with [Online's] ability to establish and maintain a market in [the] state for the sales.'"

… We conclude that the fact Online's return policy was posted for less than 11 months during the 18-month disputed period does not alter the constitutional analysis. As Online itself notes, the question for purposes of the commerce clause is the "nature and extent" of the activities in the taxing state. Here, Borders stood ready to accept returns and issue refunds for all Online merchandise purchased in California, whether or not this policy was actually posted on Online's website. All the while, Borders and Online were involved in cross-promotional activities, promoting the Borders "brand." Were we to accept Online's argument that a substantial nexus did not exist during the entire time period, the company would be free to simply promote the policy through its in-state agent and reap the benefits of that policy while avoiding the state's use tax by promoting—and then simply removing—the policy on its website….[31]

CASE QUESTIONS

1. In your view, how should this case have been decided and why?
2. Do you think companies that are aware of this case will try to lessen their connections with taxing states in order to avoid such a tax?
3. ***Ethical Consideration:*** Is it right to tax a company merely because it has a policy that anything purchased on one of its websites can be returned in its store? Is that the kind of relationship that should yield a tax?

An out-of-state web retailer might have a physical presence for tax jurisdiction purposes without having a retail store in the taxing state. In order to avoid being subject to collecting and paying a sales tax to the taxing state, an online company should be aware that other in-state activities may establish a tax nexus with the ebusiness:

- Renting an office or warehouse in the taxing state
- Holding trade shows at which employees or agents take orders from customers in the taxing state
- Using a web merchant's server
- Working with a server in the taxing state
- Licensing software to licensees in the taxing state
- Hiring agents in the taxing state
- Maintaining a business relationship with a brick-and-mortar company in the taxing state
- Failing under the market maintenance theory

Also consider the case of *Geoffrey, Inc. v. Commissioner*, involving major toy retailer Toys "R" Us. In reviewing *Geoffrey,* consider the role that intangible intellectual property assets can play in the determination of jurisdiction for purposes of ecommerce taxation. These assets, valuable in and of themselves, also have value in insofar as they help to determine significant issues, such as when sales taxes of a particular jurisdiction will be applied.

[31] *Id*, 129 Cal. App. 4th at 1196, 1199, 1201, 29 Cal. Rptr. 3d at 188, 190-91, 192 (citation omitted).

GEOFFREY, INC. v. COMMISSIONER
453 Mass. 17, 899 N.E.2d 87 (2009)

FACTS

Appellant Geoffrey, Inc. (Geoffrey) was given, and now owns, several trademarks, trade names, and service names that are associated with Toys "R" Us, Inc. Geoffrey's business consisted of licensing out these trademarks (through contracts) to various Toys "R" Us retail locations, including the one that is the subject of this case, Toys "R" Us Mass. Inc, which operated 26 Toys "R" Us locations in Massachusetts. Geoffrey had the rights to conduct inspections and oversee activities primarily to ensure that the trade names did not become generic. Geoffrey also received royalties from the retail locations throughout Massachusetts.

In 2002, during a state audit of Geoffrey, the tax commissioner discovered that Geoffrey was not filing corporate excise returns in Massachusetts and provided it with a notice of deficiency for not paying taxes on the royalties earned from the retail locations there. The basis for this tax was Massachusetts General Laws Ch. 63 § 39, which states:

> *[E]very foreign corporation, exercising its charter, or qualified to do business or actually doing business in the commonwealth, or owning or using any part or all of its capital, plant or any other property in the commonwealth, shall pay, on account of each taxable year, the [specified] excise.*[32]

Geoffrey filed an application for abatement, claiming that it was not required to pay taxes in Massachusetts on the royalties since it did not have a physical presence in the state. The commissioner and the board denied the application. Geoffrey filed appeal to the appellate tax board, which affirmed the denial. The tax board's reasoning in denying the application was that Geoffrey had a substantial nexus with the state and it purposefully entered into that state to reap economic benefits, factors that would allow an income tax to be imposed on it.

JUDICIAL OPINION (JUDGE SPINA)

The Supreme Court of Massachusetts stated that the standard that it must apply in assessing the board's decision is that:

> *A decision by the board will not be modified or reversed if the decision "is based on both substantial evidence and a correct application of the law." We presume that a tax is constitutionally valid unless the party challenging it establishes its invalidity "beyond a rational doubt." While we give deference to the board's expertise in interpreting the tax laws of the Commonwealth, we apply our independent judgment as to both the law and the facts on constitutional issues.*[33]

The Supreme Court of Massachusetts held that a physical presence is not necessary in order for a state to impose an income tax on interstate commerce. Rather, only a substantial nexus is required. The court specifically held that an income tax may be imposed when the following is fulfilled: (1) the tax is applied to an activity with a substantial nexus in that state, (2) it is fairly apportioned, (3) it does not discriminate against interstate commerce, and (4) it is fairly related to the services provided by the state. To establish a substantial nexus, the business activities must be more than a mere slight presence, and if economic activities are performed in-state by the business's personnel or on the business's behalf, a substantial nexus can be established. In this case, Geoffrey's trademarks appeared in many places in the Massachusetts locations including on signs, packaging, and store displays.

> *Here, Geoffrey engaged in business activities with a substantial nexus to Massachusetts during the tax years at issue. Geoffrey entered into contractual relationships, in the form of licensing agreements, with TRUMI and Baby Superstore and permitted those entities to use the trademarks exclusively in Massachusetts; Geoffrey encouraged Massachusetts consumers to shop at Toys "R" Us, Kids "R" Us, and Babies "R" Us through an implicit promise, manifested by the trademarks, that the products at those stores would be of good quality and value; Geoffrey relied on employees at TRUMI to maintain a positive retail environment, including store cleanliness and proper merchandise display; and Geoffrey reviewed licensed products and materials that would be sold in the Commonwealth to ensure high standards and to maintain its positive reputation with Massachusetts consumers, thereby generating continued business and substantial profits. Geoffrey's annual royalty income from retail stores in*

(*Continued*)

[32] 899 N.E.2d 87, 91 (Mass. 2009).

[33] *Id.* at 91 (citations omitted).

the Commonwealth for the tax year ending February 1, 1997, was $5,928,567, and it increased to $7,423,420, by the tax year ending February 3, 2001. Based on the findings of the board, we conclude that Geoffrey's activities established a substantial nexus with Massachusetts, and, therefore, the assessment of the corporate excises, pursuant to G.L. c. 63, § 39., for the tax years at issue comported with the commerce clause.[34]

CASE QUESTIONS

1. Based on the standards articulated in *Geoffrey, Inc.*, should the state be allowed to impose a tax on the income that Geoffrey receives from royalties from the Massachusetts chain stores?
2. It seems as though all Geoffrey would have to do in order to prevent taxation in Massachusetts would be to license out the name for a set price and then not have anything else to do with the locations there. Why would Geoffrey hesitate to do that?
3. ***Ethical Consideration:*** Did the *Geoffrey* court reach the right decision? Should a company have to pay income taxes in a state where it receives royalties even though it has no presence there? Surely the company pays federal and state taxes on the income it receives. Should it have to first pay royalty taxes in Massachusetts?

The *Geoffrey* and *Borders* cases are particularly interesting as they show how courts have construed the law so as to find a nexus between the business and the state, thus allowing states to order the businesses to collect the tax. These issues are not likely to go away anytime soon. In fact, as state governments continue to face budgetary challenges, these issues are likely to become the subject of increasing attention.

EXHIBIT 11.3 For the Month of August 2008 and Previous Months

ST-9

SM

MASSACHUSETTS DEPARTMENT OF REVENUE
MONTHLY SALES AND USE TAX RETURN
YOU MUST FILE THIS FORM EVEN THOUGH NO TAX MAY BE DUE.

FEDERAL IDENTIFICATION NUMBER	BE SURE THIS RETURN COVERS THE CORRECT PERIOD ☐ Check here if EFT payment.	FOR MONTH

IF ANY INFORMATION IS INCORRECT, SEE INSTRUCTIONS.

☐ Check if final return and you wish to close your sales tax account.

Return is due with payment on or before the 20th day of the month following the month indicated above. Make check payable to Commonwealth of Mass. **Mail to: Mass. Dept. of Revenue, PO Box 7039, Boston, MA 02204-7039.**

I declare under the penalties of perjury that this return (including any accompanying schedules and statements) has been examined by me and to the best of my knowledge and belief is a true, correct and complete return.

Signature Title Date

Note: An entry must be made in each line. Enter "0," if applicable.

1. GROSS SALES		
2. SALES FOR RESALE/ EXEMPT SALES OR OTHER ADJUSTMENTS		
2A. SALES OF MATERIALS, TOOLS AND FUEL		
2B. SALES OF MACHINERY AND REPLACEMENT PARTS		
3. TOTAL NONTAXABLE SALES (ADD LINES 2, 2A AND 2B)		
4. TAXABLE SALES (SUBTRACT LINE 3 FROM LINE 1; ZERO IF NEGATIVE)		
5. USE TAX PURCHASES		
6. TOTAL TAXABLE AMOUNT (ADD LINE 4 AND LINE 5)		
7. TOTAL TAXES (LINE 6 × .05)		
8. PENALTIES AND INTEREST		
9. TOTAL AMOUNT DUE (ADD LINE 7 AND LINE 8)		

Note: Lines 2A and 2B are for the sales of items becoming part of property sold or used directly in industrial or certain other production. These items are not to be used for income deductions.

[34] *Id.* at 93.

EXHIBIT 11.4 Summary of State ECommerce Sales Tax Laws

STATE	ENACTED OR PROPOSED	DATE
New York	Enacted; being challenged in court	2008
North Carolina	Enacted	2009
Rhode Island	Enacted; a repeal has been proposed	2009
Colorado	Enacted	2010
California	Under consideration	N/A
Connecticut	Under consideration	N/A
Illinois	Under consideration	N/A
Maryland	Under consideration	N/A
Virginia	Under consideration	N/A
Vermont	Under consideration	N/A

Recent Developments

The battle for ecommerce sales tax revenues assumed a new sense of urgency in 2009 and 2010, as the economic crisis left many states in desperate need of sales tax revenues. After doing nothing about the issue for a decade, many states started to reconsider taxation on ecommerce as a revenue-generating mechanism out of budget desperation. Many states, including California, Connecticut, Illinois, Maryland, Vermont, and Virginia, held hearings to consider legislation that would require operators of ecommerce sites to charge consumers local sales tax on purchases.

Some states have already enacted legislation. New York has had legislation in place since 2008, and the measure is being challenged in court. North Carolina and Rhode Island have had laws in place since 2009, but in Rhode Island, some lawmakers proposed a repeal of the measure. In early 2010, Colorado passed a law that requires ecommerce sites to either collect sales tax or share information with the state about purchases made by residents. When Colorado directed Amazon.com to notify all state residents of their tax owed on Amazon purchases, the company responded by unplugging all the affiliate marketers in Colorado from its system. That way, Amazon could argue that it did not have a physical location in the state and thus did not need to pay sales tax. Thus, these kind of measures can and have had a negative impact on small businesses, such as the affiliate marketers, who have relied upon Amazon for much of their business.

New York's law is particularly interesting. The legislation counts in-state marketing affiliates (people or companies who earn a fee for providing links to online retailers on their own website) as local sales agents, thus giving the sites physical presence in the state. Amazon challenged the law in court, contending that the affiliates are advertising channels, not sales agents, and do not constitute a physical presence in the state on the part of Amazon.

Regulation of Content

User-Generated Content

User-generated content (UGC) refers to various kinds of content created by end-users (as opposed to a website operator, for example) and made publicly available. There are

many examples of UGC in the Web 2.0 world. Some common examples include customer reviews, social networking content, videos and photos uploaded by users, blog posts, and wikis.

For many websites, UGC constitutes only a portion of content. For example, on many ecommerce websites, the majority of content is prepared by website operators, but the site also displays user reviews of the products being sold submitted by visitors to the website. On other sites, UGC is the primary content of the site. Examples of such sites include Flickr (a photo sharing site), Facebook (a social networking site), YouTube (a video sharing site), TripAdvisor (a site where users can share travel information, including reviews of hotels and other travel-related goods and services), Wikipedia (a research resource created with UGC), Second Life (a social gaming site), and Twitter (a social communication service). UGC is even contributing to the news. In 2006, major news network CNN launched iReport, a project designed to bring UGC to CNN. Other news organizations, including Fox News and Sky News, have followed suit.

UGC has had profound implications on the cyberworld and, by extension, on all of society. As an indication of the significance, in 2006 Time magazine's Person of the Year was "you," meaning all who contribute UGC to the web. The introduction of UGC represents a shift from a world in which large media organizations dominated the content available to everyone, to one in which amateurs have sufficient opportunities and facilities to publish their own content and make it available to large audiences. UGC also has made online communications more conversational. In the not–so-distant past, the media was one voice speaking to many. By 2010, there was much more of a two-way process, with individuals posting UGC to the Web and also commenting upon UGC posted by other users.

Often UGC is partially or totally monitored by website administrators. Monitoring can be undertaken for a number of purposes, including to avoid offensive content or language, copyright infringement issues, and to determine if the content posted is relevant to the site's general theme.

While UGC is an important part of the online world, it is not without its legal risks and concerns. Content created by others, including website users, can, for instance, give rise to intellectual property concerns, violate individual privacy rights, result in criminal liability, and raise other concerns. Website operators can attempt to mitigate the potential risks of UGC by implementing systems for reviewing UGC before it is posted, but for most companies this is not practical. Moreover, even the most thorough review policies and procedures are incapable of detecting all unacceptable UGC. Fortunately, as will be discussed herein, certain laws provide some protection against liability for some forms of UGC. Moreover, websites can also protect themselves with the use of appropriate agreements and disclaimers. Many websites aim to protect themselves through the use of comprehensive provisions in their website agreements. Consider, for instance, the following provision from TripAdvisor.com

> *TripAdvisor takes no responsibility and assumes no liability for any Content posted, stored or uploaded by you or any third party, or for any loss or damage thereto, nor is TripAdvisor liable for any mistakes, defamation, slander, libel, omissions, falsehoods, obscenity, pornography or profanity you may encounter. As a provider of interactive services, TripAdvisor is not liable for any statements, representations or Content provided by its users in any public forum, personal home page or other Interactive Area. Although TripAdvisor has no obligation to screen, edit or monitor any of the Content posted to or distributed through any Interactive Area, TripAdvisor reserves the right, and has absolute discretion, to remove, screen or edit without notice any Content*

posted or stored on the Site at any time and for any reason, and you are solely responsible for creating backup copies of and replacing any Content you post or store on the Site at your sole cost and expense.[35]

As noted above, UGC can give rise to privacy concerns. By posting UGC, users may inadvertently disclose more information about themselves and/or others than they had intended to. This can make users vulnerable to range of harms, including identity theft. UGC can also give rise to privacy issue when individuals post the private photographs and other content of third parties.

Operators of websites on which users are permitted to post UGC may also face liability risks arising out of the nature of the content. One of most significant risks is copyright infringement. Given the in-depth examination of these issues in Chapter 5, we will not focus on them in too much detail here. However, issues particular to UGC are worthy of some discussion. Consider, for instance, if you host a site where users are invited to share their opinions on movies, music, and the like. What if, when commenting upon a certain video, a website user posts the video, without permission of the rights holder?

The key law for analyzing the website operator's liability in such a situation is the Digital Millennium Copyright Act (DMCA). Section 512 of the DMCA establishes a safe harbor under which an Internet service provider (ISP) can escape liability for copyright infringement, as long as the ISP meets certain conditions. Of course, the ISP seeking immunity must not have been involved in the infringement. Additionally, ISPs are required to adopt a special take-down policy, which allows individuals to respond to alleged copyright violations. If the individual moves "expeditiously" to remove the infringing material, he or she usually avoids liability. When the company removes the infringement, it is then required to notify the user that their material has been taken down. If the user then submits a counter-notification claiming a "good faith belief" that the material is not infringing, the company must put the material back online unless the original company claiming the infringement brings a suit against the user.

Of course, copyright infringement is not the only potential liability about which websites hosting UGC must be concerned. In the context of third-party copyright violations, it is important to consider the liability issues between the content provider and the ISP. There are two distinct models of liability: the "publishing information doctrine" and "storing information doctrine." According to the former view, ISP controls, or at least has the ability to control, the content published by virtue of the fact that the user is using its services. In other words, the ISP has the editorial control to take down and monitor content posted online. In order to establish secondary liability it is pivotal to evaluate the level of control practiced by the ISP. The more control the ISP has before the content is posted, the more likely it will be subjected to greater liability, but it is also greatly decreases the risk objectionable material will be posted on the Internet. The latter view applies to situations in which the ISP acts as a mere host, lacking any editorial role to the content posted online. Even though the ISP might have awareness of the content run by using their services, it cannot monitor or modify posted information.

UGC can also give rise to defamation claims, a topic discussed in the following section.

Website Liability and the Communications Decency Act

The **Communications Decency Act** of 1996[36] **(CDA)** plays a very important role in insulating website operators from liability for UGC. To understand the role and importance of the CDA, one can look at traditional common-law principles. Under those

[35]http://www.tripadvisor.com/pages/terms.html.

[36]47 U.S.C. § 230.

principles, a person who publishes a defamatory statement by another would bear the same liability for the statement as if he or she had initially created it. Accordingly, a book publisher or a newspaper publisher could be held liable for anything that appeared within its pages. This common law rule is based on the notion that a publisher has the knowledge, opportunity, and ability to exercise editorial control over the content of its publications.

Conversely, under common law, the liability of *distributors* of content is much more limited. Generally, distributors, such as newsstands, bookstores, and libraries, are not held liable for the content of the material they distribute. The theory behind this principle is clear: It would be difficult, if not impossible, for distributors to read every publication before they sell or distribute it.

In the early days of the Internet, a number of lawsuits were brought that tested how websites should be classified—as distributors or publishers. The early cases in this area, such as *Cubby v. CompuServe, Inc.*[37] and *Stratton Oakmont v. Prodigy*,[38] resulted in an interesting scenario. Efforts by online information providers to restrict or edit user-submitted content faced a much higher risk of liability if the provider failed to eliminate all defamatory material than if it simply did not try to control or edit the content of third parties at all.

This eventually led to the passage of the Communications Decency Act. Of most relevance is Section 230, which provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" and further that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."

Section 230 of the CDA applies to "interactive computer service[s]," a term that is defined broadly to include any "information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." Courts have interpreted this term to include a wide variety of Internet services, including websites, blogs, forums, and listservs.

Section 230 has most frequently been applied to bar defamation-based claims. However, immunity is not limited to defamation or speech-based torts. Courts have applied Section 230 immunity to bar claims such as invasion of privacy and misappropriation. In a case brought against MySpace, the claimant asserted that MySpace was negligent for failing to implement age verification procedures and to protect a 14-year–old girl from sexual predators.

DOE v. MYSPACE, INC.
528 F.3d 413 (5th Cir. 2008)

The Fifth Circuit Court of Appeals considered whether the social networking site MySpace could be held liable for negligently failing to confirm that a user, who was assaulted by a predator she met through the website, was actually of the age required to create a profile on MySpace's website.

FACTS

In 2005, at age 13, Julie Doe lied about her age, representing that she was 18 years old, and created a profile on MySpace.com.

(*Continued*)

[37]776 F. Supp. 135 (S.D.N.Y. 1991).

[38]23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

MySpace.com membership is free to all who agree to the Terms of Use. To establish a profile, users must represent that they are at least fourteen years of age. The profiles of members who are ages 14 and 15 are automatically set to "private" by default, in order to limit the amount of personal information that can be seen on the member's profile by MySpace.com users who are not in their existing friends network, and to prevent younger teens from being contacted by users they do not know.

When Julie claimed she was 18, the MySpace website permitted her to circumvent all safety features of the site and her profile was made public. This enabled 19-year-old Pete Solis to contact Julie in April 2006 when she was 14. The two communicated offline on several occasions after Julie provided her telephone number. They met in person in May 2006, and, at this meeting, Solis sexually assaulted Julie.

Julie's mother, Jane Doe, sued Solis as well as MySpace, Inc., its parent company, News Corporation (collectively "MySpace") on her own behalf and on behalf of her daughter, alleging that MySpace failed to implement basic safety measures to prevent sexual predators from communicating with minors on its website. MySpace then submitted a motion to dismiss, which was granted by the district court. The Does then appealed to the Fifth Circuit Court of Appeals.

JUDICIAL OPINION (CIRCUIT JUDGE CLEMENT)

The court first determined the scope and purpose of § 230 of CDA.

> *The Does now appeal the district court's dismissal of their claims for negligence and gross negligence, arguing that § 230(c)(1) of the CDA is inapplicable here because their claims do not implicate MySpace as a "publisher" protected by the Act and because MySpace not only published but was also partially responsible for creating the content of the information that was exchanged between Julie and Solis.*
>
> *… Congress enacted the CDA for several policy reasons, including "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." To achieve that policy goal, Congress provided broad immunity under the CDA to Web-based service providers for all claims stemming from their publication of information created by third parties, referred to as the "Good Samaritan" provision.…*
>
> *Courts have construed the immunity provisions in § 230 broadly in all cases arising from the publication of user-generated content … Acknowledging that the immunity provision in § 230(c)(1) of the CDA causes "Internet publishers [to be] treated differently from corresponding publishers in print, television and radio," the Ninth Circuit held that "[u]nder § 230(c), … so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process."*
>
> *… Parties complaining that they were harmed by a Web site's publication of user-generated content have recourse; they may sue the third-party user who generated the content, but not the interactive computer service that enabled them to publish the content online.*[39]

The court then addressed the Does' argument that the CDA was inapplicable to their case.

> *The Does appear to agree with the consensus among courts regarding the liability provisions in § 230(c)(1). They argue, however, that their claims against MySpace do not attempt to treat it as a "publisher" of information; therefore, they argue that § 230 does not immunize MySpace from their claims and state tort law applies in full effect.*
>
> *… The Court, however, finds this artful pleading to be disingenuous. It is quite obvious the underlying basis of Plaintiffs' claims is that, through postings on MySpace, Pete Solis and Julie Doe met and exchanged personal information which eventually led to an in-person meeting and the sexual assault of Julie Doe. If MySpace had not published communications between Julie Doe and Solis, including personal contact information, Plaintiffs assert they never would have met and the sexual assault never would have occurred. No matter how artfully Plaintiffs seek to plead their claims, the Court views Plaintiffs' claims as directed toward MySpace in its publishing, editorial, and/or screening capacities.*
>
> *The Does do not present any caselaw to support their argument. In fact, they rely upon the same line of cases listed above but point to § 230(c)(1)'s grant of immunity to publishers of third-party content as*

(*Continued*)

[39]528 F.3d 413, 417, 418-19 (5th Cir. 2008) (citations omitted).

evidence that their claims are somehow different. Other courts, however, have examined pleadings similar to the Does' and have reached the same conclusion as the district court.[40]

Finally, the court addressed a claim not previously raised by the Does in district court.

The Does further argue for the first time on appeal that MySpace is not immune under the CDA because it partially created the content at issue, alleging that it facilitates its members' creation of personal profiles and chooses the information they will share with the public through an online questionnaire. The Does also contend that MySpace's search features qualify it as an "information content provider", as defined in the CDA: "The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."

Nothing in the record, however, supports such a claim; indeed, Julie admitted that she lied about her age to create the profile and exchanged personal information with Solis. In the February 1, 2007 hearing before the district court, the Does admitted that Julie created the content, disclosing personal information that ultimately led to the sexual assault, but stressed that their cause of action was rooted in the fact that MySpace should have implemented safety technologies to prevent Julie and her attacker from meeting.

At no time before filing their appeal in this Court did the Does argue that the CDA should not apply to MySpace because it was partially responsible for creating information exchanged between Julie and Solis. Because the Does failed to present this argument to the district court, they are barred from making this argument on appeal.[41]

CASE QUESTIONS

1. Did the court of appeals determine that there were grounds for holding MySpace liable in this case?
2. How broad did the court consider the CDA to be in creating immunity for ISP?
3. In addition to the court's finding that MySpace fit into the immunity provision of the CDA, do you think there are other reasons the court rejected the Does' claim?

Although Section 230 of the CDA explicitly exempts from its coverage criminal law, communications privacy law, and "intellectual property claims," there is still a broad range of claims for which the CDA will provide protections. In order to take advantage of those protections, operators of websites should familiarize themselves with the suggested best practices outlined in Exhibit 11.5.

EXHIBIT 11.5 Summary of CDA Best Practices

- A website that passively hosts third-party content will be protected under § 230 of the CDA.
- A website that exercises traditional editorial functions over user-submitted content, such as deciding whether to publish, remove, or edit material, will not lose immunity unless the edits materially alter the meaning of the content.
- A website operator that prescreens objectionable content or corrects, edits, or removes content, will not lose its immunity.
- A website operator that encourages or pays third parties to create or submit content will not lose its immunity.
- A website that uses drop-down forms or multiple-choice questionnaires should be cautious of allowing users to submit information through these forms that might be deemed illegal.
- Subject to limited exceptions, § 230 of the CDA provides broad protection from liability from a number of different claims.

[40] *Id.* at 419-20.

[41] *Id.* at 420, 422 (citation omitted).

The Third Circuit Court of Appeals was asked to consider a very interesting case involving the CDA. Even though this case did not reverse the trend of the CDA providing strong liability protection for website operators, it did find that website operators could be liable for failing to remove website content when they have promised to do so.

BARNES v. YAHOO!, INC.
570 F.3d 1096 (9th Cir. 2009)

In the case of *Barnes v. Yahoo!, Inc.*, the Ninth Circuit Court of Appeals considered whether a computer service provider can be held liable for negligently failing to remove unauthorized material about the plaintiff posted by a third party.

FACTS

In 2004, Barnes, an Oregon resident, broke up with her boyfriend. He responded by posting indecent profiles of her on a website run by Yahoo!. According to Yahoo!'s Member Directory, "[a] public profile is a page with information about you that other Yahoo! members can view. You[r] profile allows you to publicly post information about yourself that you want to share with the world. Many people post their age, pictures, location, and hobbies on their profiles." After the profiles were posted, men who Barnes's ex-boyfriend had contacted using her identity began to harass her.

In accordance with Yahoo! policy, Barnes mailed Yahoo! a copy of her photo ID and a signed statement denying her involvement with the profiles. She then requested their removal. One month later, Yahoo! had not responded and Barnes again requested that Yahoo! remove the profiles. The following month, when the profiles were still not removed, Barnes sent Yahoo! two more requests to have the profiles removed. Only then, the day before a local news program was preparing to broadcast a report on the incident, did a Yahoo! representative call Barnes and ask her to fax directly the previous statements she had mailed. Barnes was told that the representative would "personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it."

Barnes took no further action regarding the profiles and the trouble they had caused. Following another two months without action by Yahoo!, Barnes filed suit against Yahoo! in Oregon state court. After Barnes initiated her suit, the profiles were permanently removed from Yahoo!'s website. The court was asked to find that Yahoo! was negligent in removing the profiles. Yahoo! Claimed that the Communications Decency Act, barring courts from treating certain Internet service providers as publishers or speakers, protected Yahoo! from liability. The lower court granted Yahoo!'s motion to dismiss, and the plaintiff appealed to the Court of Appeals for the Ninth Circuit.

JUDICIAL OPINION (JUDGE O'SCANNLAIN)

The court first addressed whether § 230(c)(1) of the Communications Decency Act rendered it immune from liability for the content that Barnes's former boyfriend had posted. The section states: "One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of the other's person or things, is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking …." Initially, the court recognized two specific purposes for the enactment of the statute.

> *We have recognized in this declaration of statutory purpose two parallel goals. The statute is designed at once "to promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material."*[42]

The court then considered whether Yahoo! fell within the protected immunity for publishers or speakers of third-party content.

> *[C]ourts must ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a "publisher or speaker." If it does, section 230(c)(1) precludes liability.*
> *… Subsection (c)(1), by itself, shields from liability all publication decisions, whether to edit, to remove, or to post, with respect to content generated entirely by third parties.*

(*Continued*)

[42]570 F.3d 1096, 1099-1100 (9th Cir. 2009) (citation omitted).

[T]he duty that Barnes claims Yahoo violated derives from Yahoo's conduct as a publisher-the steps it allegedly took, but later supposedly abandoned, to depublish the offensive profiles. It is because such conduct is ***publishing conduct*** *that we have insisted that section 230 protects from liability "any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online."*

[S]ection 230(c)(1) precludes courts from treating [I]nternet service providers as publishers not just for the purposes of defamation law, with its particular distinction between primary and secondary publishers, but in general. The statute does not mention defamation, and we decline to read the principles of defamation law into it.[43]

After dismissing Barnes's claim under CDA § 230 (c)(1), the court considered whether she could make a claim under an alternative legal theory.

… Barnes's complaint could also be read to base liability on section 90 of the Restatement (Second) of Contracts, which describes a theory of recovery often known as promissory estoppel.

… The "principal criteria" that determine "when action renders a promise enforceable" under this doctrine are: "(1) a promise[;] (2) which the promisor, as a reasonable person, could foresee would induce conduct of the kind which occurred[;] (3) actual reliance on the promise[;] (4) resulting in a substantial change in position."

… Contract liability here would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication.

[W]e conclude that, insofar as Barnes alleges a breach of contract claim under the theory of promissory estoppel, subsection 230(c)(1) of the Act does not preclude her cause of action.[44]

CASE QUESTIONS

1. How can you explain the difference between the court's denial of Barnes's claim to hold Yahoo! liable as the publisher of a third-party act and its willingness to accept Barnes's quasi-contractual claim under a promissory estoppel theory?
2. ***Ethical Consideration:*** What do you think was the underlying reason for the court finding that the CDA permitted Yahoo! to avoid liability in this case? Should the CDA help to insulate website operators from liability?
3. Assume that, after remand, the district court finds Yahoo! is not liable under the plaintiff's promissory estoppel claim. Would the Ninth Circuit affirm?

Summary

The foregoing cases show how courts and the government regulate the Internet in several different aspects. We analyzed the extent to which courts will interfere with online activities in terms of taxation, antitrust regulatory liability, and content found on the Internet. Additionally, the topics were visited from different viewpoints, including that of companies in terms of corporate liability and state-level taxation when business is done over the Internet. We looked at criminal liability and what actions on the Internet can subject a person to criminal liability. What we have seen as an emerging trend is that courts are not as hesitant as some might expect when it comes to enforcing regulations on Internet users. Does this mean that the government will increase its regulatory behavior? Only time will tell.

[43] *Id.* at 1102, 1103, 1104, 1105 (citation omitted).

[44] *Id.* at 1106, 1109 (citation omitted).

Key Terms

nonrival goods, p. 333
nonexcludable goods, p. 333
cybersquatting, p. 334
antitrust, p. 336
Sherman Act, p. 336
Clayton Act, p. 336
price discrimination, p. 336
interlocking directorates, p. 336
tying, p. 337
Internet Service Providers (ISPs), p. 340
net neutrality, p. 340
wireless spectrum management, p. 343
sales tax, p. 344
nexus, p. 345
use tax, p. 346
user-generated content (UGC), p. 352
Communications Decency Act (CDA), p. 354

Manager's Checklist

- *Managers of ebusinesses must be aware of the impact of law, market-forces, funding, and technology on the regulation of their businesses. The regulation of ecommerce and other online conduct continues to evolve and, as a result, companies engaging in online transactions must remain vigilant about changes that will impact their businesses.*
- *The antitrust laws are intended to limit restraints on trade, such as price fixing, monopolization, etc. Agreements that reduce competition in the marketplace need to be addressed in an Internet context. Although the impact of antitrust laws in the online environment is relatively new, the potential for anticompetitive practices is significant. Businesses must carefully look at any business arrangement that affects competition with respect to prices and product or services information.*
- *Net neutrality is the idea that all information going across the Internet should be treated equally, but in reality, some information, such as online games, creates more Internet congestion. The debate over net neutrality is being played out in Congress and the marketplace. Although it remains to be seen whether Internet information will be regulated by the government or whether market forces will work it out, multitier users are likely going to be required to pay extra fees. From the standpoint of an Internet business manager using data-rich content, it is smart to be aware that the cost of Internet usage might be higher.*
- *Operators of ecommerce businesses must stay abreast of changes and be prepared to adjust their operations when necessary. Noncompliance with tax law can result in substantial penalties for the ebusiness. Managers should work closely with their accountants and tax advisors to ensure that they are collecting tax in a manner that complies with applicable legal requirements.*
- *Although the general trend is to limit the liability of website operators for defamatory statements posted by their end users, website operators should nonetheless have an aggressive antidefamation policy and act to remove offending information whenever it is found.*

Questions and Case Problems

1. Plaintiff LiveUniverse, Inc. (LiveUniverse), and Defendant MySpace, Inc. (MySpace) are social networking companies that operate websites on the Internet allowing users to create profiles, view friends' profiles, and perform other social activities. MySpace created a system that does not allow users to view videos posted through LiveUniverse's website, vidilife.com, and it also deleted any references by MySpace users to the vidilife website. LiveUniverse alleges that these actions violate the Sherman Act by monopolizing, or attempting to monopolize, the market for social networking. LiveUniverse filed a complaint in the District Court for the Central District of California.

According to the district court, in order to establish a claim for monopolization, one must prove three elements: "(i) possession of monopoly power in the relevant market, (ii) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident, and (iii) causal antitrust injury." Possession of monopoly power in a relevant market means that the company has the power to exclude competition in an identified market of goods or services in a certain geographic region by owning dominant shares of the market and putting up barriers to entry. The second monopolization prong requires that

the alleged violator of the Act engaged in exclusionary conduct. This means that its actions harmed the competitive process *and* thereby harmed consumers. Mere harm to one of its competitors is not enough to show monopolization. Finally, one must show causal antitrust injury, which means injury to the competitive process that flows from the defendant's anticompetitive actions. If one cannot establish that the defendant's actions were anticompetitive by satisfying the second prong, the third prong is obviously impossible to prove.

Based on the foregoing, discuss whether or not LiveUniverse should be able to claim monopolization by MySpace on the market for social networking. What should the district court conclude, and why?[45]

2. Defendant Consumeraffairs.com, Inc. (Consumeraffairs) operates a website that allows consumers to comment on their experiences with various businesses, goods, and services. The subject of this suit is a car dealership, Nemet Chevrolet (Nemet), the plaintiff, which claimed it was defamed by Consumeraffairs by several negative postings about Nemet on Consumeraffairs's website. Nemet filed suit in the United States District Court for the Eastern District of Virginia. Consumeraffairs moved to dismiss the case on the ground that it was barred by Section 230 of the CDA, which precludes plaintiffs from holding interactive computer service providers liable for publication of information created by a third party. The motion to dismiss was granted and the case was appealed to the United States Court of Appeals for the Fourth Circuit.

On appeal, Nemet contended that Consumeraffairs was an *information content* provider, which would preclude it from receiving immunity under the CDA. The basis of this allegation is the fact that some of the postings had no apparent author, such that allegedly Consumeraffairs must have been the author, thereby making it an information content provider.

In order to overcome a motion to dismiss, a plaintiff must make more than mere conclusory statements and bare assertions.

Is Nemet's claim that Consumeraffairs should not have immunity, valid? Is the fact that Nemet cannot ascertain the author of the posts enough to support its allegation that Consumeraffairs is the author—thus categorizing Consumeraffairs as an information content provider that does not have immunity?[46]

3. The Jenkins Act, a federal law, requires any out-of-state sellers of cigarettes to submit customer information to the states in which it sells its cigarettes. The purpose of the Act is to ensure that purchasers of cigarettes pay the appropriate taxes when purchasing. The Racketeer Influenced and Corrupt Organizations Act (RICO), another federal law, provides for criminal penalties for racketeering activities, which includes mail and wire fraud.

In this case, Plaintiff, the State of New York, brought an action based on these two federal statutes against Hemi Group (Hemi), a New Mexico based company, for not filing the Jenkins Act report when selling cigarettes over the Internet to customers in New York. New York alleged that the failure to file the report constituted mail and wire fraud under RICO. The District Court for the Southern District of New York dismissed the action. The Court of Appeals for the Second Circuit vacated the judgment and remanded the case. It was appealed to the Supreme Court of the United States.

In order to establish a claim based on RICO, New York would have to show that the taxes that it should have received from the customers purchasing the cigarettes was "by reason of" Hemi not complying with the Jenkins Act reporting requirements and thereby violating RICO. To satisfy the requirement of "by reason of," New York would have to show that it was not only a "but for" cause, but also a proximate cause of its lost taxes. *Decide and state your reasons why or why not the Supreme Court should affirm the judgment of the district court dismissing New York's claim of Hemi's violation of RICO.*[47]

4. In a stated effort to enforce laws concerning child pornography, the United States Department of Justice asked a number of leading Internet companies, including Yahoo!, Google, America

[45] *LiveUniverse, Inc. v. MySpace, Inc.*, No. CV 06-6994 AHM, 2007 WL 6865852 (C.D. Cal. June 5, 2007).

[46] *Nemet Chevrolet Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250 (4th Cir. 2009).

[47] *Hemi Group, LLC v. New York*, ___ U.S. ___, 130 S. Ct. 983 (2010).

Online and Microsoft to turn over records concerning Internet users' online searches. Although Yahoo!, America Online and Microsoft complied with the request, Google resisted, choosing to fight the government's subpoena in court. This case shows how companies in private industry are often called upon to provide information to assist the government in its law enforcement and antiterrorism activities. *Consider and discuss whether the government should make such requests of companies operating in the private sector and whether companies should comply with those requests, even when compliance requires the company to breach privacy promises made to its customers.*

5. Users of the popular Internet website Craigslist are able to post advertisements for housing that permit statements regarding the preference, limitation, or discrimination of others based on race, religion, sex, or family status. The Fair Housing Act (FHA), however, prohibits making, printing, or publishing a notice, statement, or advertisement for sale or rental of dwellings indicating preference, limitation, or discrimination based on protected classes. As such, Chicago Lawyers Committee for Civil Rights Under Law, Inc. brought suit against Craigslist alleging a violation of the FHA. In defense, Craigslist claimed that it was immune from liability based on Section 230(c)(1) of the CDA, which protects interactive computer services from liability for unlawful third-party content. *Should Craigslist be subject to liability for FHA violations? Why or why not? Cite to appropriate legal principles when explaining your answer.*[48]

Additional Resources

- Educause Resources on Net Neutrality: http://www.educause.edu/Resources/Browse/Net%20Neutrality/31666
- Electronic Frontier Foundation: Legal Guide for Bloggers: http://www.eff.org/issues/bloggers/legal
- Federal Communications Commission Resources on Broadband Network Management: http://www.fcc.gov/broadband_network_management
- Federal Trade Commission: Business Guide to Consumer Protection Issues: http://www.ftc.gov/bcp/business.shtm

[48] *Chicago Lawyers Committee for Civil Rights Under Law, Inc. v. Craigslist*, 519 F.3d 666 (7th Cir. 2008).