1

INTRODUCTION TO THE STUDY OF CYBERSPACE LAW

As with any course, we must begin with the question: Why study this subject matter? Is it worth studying? What do we hope to gain? This is especially true with respect to cyberspace law because not only is the area relatively new, but it is constantly changing and evolving. This section begins by providing an overview of how the Internet works. This overview is deliberately short and general. The study of cyberspace law does not require a detailed understanding of computer or telecommunications technology. Like the study of law in general, the focus is on how society is responding and should respond to certain activities and events. This section then introduces the reader to three of the principal approaches to the question of why study cyberspace law, and concludes by introducing the reader to the approach taken by this casebook.

A. INTERNET BASICS

RAYMOND SHIH RAY KU
OPEN INTERNET ACCESS AND FREEDOM OF SPEECH: A FIRST AMENDMENT CATCH-22

75 Tul. L. Rev. 87 (2000)

In essence, the Internet is simply a collection of computers, a network, in which the computers are capable of communicating with each other. What makes the Internet special is its reach as the largest network in the world. . . . Through this network you can send e-mail to friends and colleagues, do research, play computer games with people from around the world, shop, read the *New York Times*, listen to radio stations, and watch video programming. All of this is made possible by shared communication protocols, such as the Transmission Control Protocol (TCP) and Internet Protocol (IP) or

TCP/IP, which allows information to be transmitted quickly from computer to computer and the hardware that links the computers together.

1. TCP/IP Protocols

The TCP/IP protocols break down information transmitted to the Internet into packets and reassemble it at its destination. This allows the Internet to operate as a packet-switched network where the various data packets may travel different routes to reach the same destination. This design allows information to be transmitted through the Internet at faster speeds than circuit-switched networks [like a traditional telephone line], where, once a connection is made, that part of the network is dedicated only to that connection. [Packet-switched networks monopolize available wire space only for the time it takes to transmit the individual packet of information. Originally designed by the United States military as a means of communicating in the event of war, transmitting information in packets is a more efficient method of using the telecommunications infrastructure and makes it possible for information to travel from sender to recipient even if portions of the network are blocked or even destroyed.]

2. The Hardware Links

As the Internet exists today, one cannot simply plug a personal computer into the Internet through a telephone or cable line any more than one can obtain telephone or cable television service by plugging a telephone into an outlet or hooking your television up to coaxial cable. Just as you contract with the telephone or cable company for telephone and cable service, to connect to the Internet you must have an ISP. Currently, four different groups provide the vast majority of Americans with access to the Internet: federal, state, and local governments; schools; private employers; and private service providers. While government, businesses, and schools provide many individuals with access outside of the home, most do not provide service to the general public or to residential users, who must contract with a private provider. Understanding why an Internet service provider is necessary requires a brief explanation of the Internet's architecture and the method by which information is transmitted across this global network of networks.

Accessing the full resources of the Internet from a personal computer requires passing through multiple layers of hardware and telecommunications services. Imagine you are sending a friend an e-mail. First, you must prepare the e-mail on your personal computer or handheld device, and that device must typically be connected to a local area network (LAN). The connection can be established either through local wiring, as in an office, or through telephone, cable, or similar services to a local ISP. When connecting through an ISP, the ISP acts as your LAN. Once connected to the LAN, your computer interacts with the LAN's internal router/server, a more powerful computer and

switching device capable of interacting with the multiple computers in a LAN simultaneously and translating different data formats. The server acts as a repository for various data and applications that allow the user to send and retrieve information on the Internet. In the case of e-mail, the server translates your e-mail through the TCP/IP protocol and sends it as various data packets. The LAN's server, in turn, must be connected to a router. Routers connect networks and direct the flow of data on the Internet. The router looks at the Internet addresses in the data packets and sends them on the best path to the recipient.

Through routers, LANs are connected into midlevel networks or regional networks. To communicate with other LANs, each LAN must be linked together through privately leased communication services such as telephone lines, T1 lines, Integrated Services Digital Network (ISDN) lines, Digital Subscriber Lines (DSL), coaxial cable, satellite, microwave, or fiber-optic cable. These types of connections are often leased from local exchange carriers such as Pacific Bell or MCI WorldCom. If the recipient of your e-mail is within the midlevel network, a router or series of routers delivers the e-mail message to the recipient's local network server where it is reassembled and eventually downloaded onto the recipient's personal computer. If the recipient is outside the midlevel network, the data packets are sent to a Network Access Point (NAP) where they are sent along high-speed backbones, capable of transmitting data at speeds of 155 Mbps (megabits per second) and higher, to another NAP and regional network, either across the country or around the world. Consequently, what people think of as the Internet is, in reality, computer equipment and telecommunications connections representing three different layers of networks.

Given the multiple layers of the Internet, it may already be apparent that in order to access what people commonly think of as the Internet one must have access to all three layers of networks: local, regional, and national/international. More importantly, given the current architecture, access fees are inescapable. Individual users must pay an ISP to be connected to a local network. Local ISPs must pay regional ISPs, such as MidWestnet or EastCoastnet, for connecting at the regional level, and regional ISPs must pay National Backbone Providers (NBPs) such as MCI WorldCom or PSINet for national and international access. While some users — for example, universities and large corporations — avoid local ISP fees by purchasing the necessary equipment, such as a router and a modem pool, thereby becoming their own ISPs, they must ultimately pay to tap into a regional ISP. Similarly, while regional ISPs may avoid paying fees to NBPs by tapping into NAPs directly, they must then pay the NAP, which is typically run by a Regional Bell Operating Company. Therefore, given the Internet's current topography, tolls on the information superhighway are unavoidable.

In addition to the limitations upon access imposed by the Internet's architecture, access to the Internet is limited by the technology used to transmit data and connect us to the Internet. Typically, the computers and computer

networks of the Internet are physically connected together through copper wire, coaxial cable, or fiber optics. Computers can also be connected through a variety of technologies that do not require direct physical connections. The type of connection between computers and networks determines the maximum speed at which information may be transmitted. For example, regular telephone lines typically transmit data at a maximum of 56 Kbps (kilobits per second). Special leased telephone lines are capable of transmitting data at even higher speeds. For example, ISDN lines can carry data at 128 Kbps and DSL can carry data at 1.5 Mbps; T1 lines can carry data at 1.5 Mbps and T3 lines can carry data at 44 Mbps; and fiber-optic cable can carry data at 600 Mbps. Similarly, cable typically transmits data at 3 Mbps. In the near future, high-speed wireless systems promise data speeds up to 100 Mbps.

[W]hat do these differences in speed mean in practical terms? The bandwidth available to a residential user influences both Internet performance and function. In short, downloading the latest version of AOL with a traditional telephone line and 56 Kpbs modem takes approximately one hour. In contrast, with a high-speed T1 line or cable modem running at 1.5 Mbps, it would only take two minutes to download the same software. The speed of data transmission translates, therefore, into the amount of time someone must spend on-line to perform even the simplest of functions such as retrieving e-mail. Additionally, bandwidth translates into more types of informational services practically available to the residential user. At slower rates of transmission, while it is possible to change webpages, download video and music, or watch streaming programming, the process can be painfully slow, making it either unappealing or practically impossible. In contrast, the high-speed data transmission promised by cable and other services makes it possible for information providers to deliver true multimedia programming. With high-speed access, individuals can change webpages as easily as changing channels on a television. They can communicate with loved ones through telephony with audio and real-time video. Broadband Internet access would permit us to watch the latest CNN report without purchasing a special video card, listen to radio stations outside their areas of service, or download the latest hit movie for home viewing in a matter of minutes. In short, broadband technology has the potential to radically transform the ways in which we receive, send, and manipulate information.

In its current form, the Internet's infrastructure and packet-switched design carry information regardless of the computer operating system used or the applications involved. This means that computers operating under different operating systems from Palm OS to Microsoft Windows to Linux can all be linked together. Similarly, the Internet is not designed to run any particular application. Applications are the computer programs that we use to access the Internet for activities including World Wide Web surfing, e-mail,

Internet telephony, or interactive games. The Internet's open design means that anyone may write a program capable of using the Internet to share, transmit, or manipulate data. Finally, the Internet's current architecture also permits access across a wide array of platforms from supercomputers to personal computers and from electronic book readers to smartphones.

For detailed discussions of the origins of the Internet or for further explanations of how the Internet works see Preston Gralla, *How the Internet Works* (Millennium Edition, 2002); Barry M. Leiner et al., *A Brief History of the Internet*, at *http://www.isoc.org/internet/history/brief.shtml*; David Post, *In Search of Jefferson's Moose: Notes on the Study of Cyberspace*, at 24-30 (2009).

In recent years, while the basic operation of the Internet has remained unchanged, the technologies utilized for transmitting information at ever greater speeds have developed at a rapid pace, causing issues for regulators of telecommunications and related services, such as the Federal Communications Commission. For a recent discussion of these developments, both technological and regulatory, see Daniel Spulber & Christopher Yoo, *Rethinking Broadband Internet Access*, 22 Harv. J.L. & Tech. 1 (2008).

B. The Study of Cyberspace Law

Because the Internet is a medium for communication, should one study "Internet Law" or should one study courses like contracts, property, and torts and explore how the doctrines developed in those "substantive" fields apply to this new technology? Is there such a thing as Internet or cyberspace law? What does the study of cyberspace law have to offer?

Frank H. Easterbrook
Cyberspace and the Law of the Horse

1996 U. Chi. Legal F. 207

When he was dean of this law school, Gerhard Casper was proud that the University of Chicago did not offer a course in "The Law of the Horse." He did not mean by this that Illinois specializes in grain rather than livestock. His point, rather, was that "Law and . . ." courses should be limited to subjects that could illuminate the entire law. . . .

. . . We are at risk of multidisciplinary dilettantism, or, as one of my mentors called it, the cross-sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds. . . . Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. . . . The blind are not good trailblazers.

Dean Casper's remark had a second meaning — that the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still

more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students — better, even, for those who plan to go into the horse trade — to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses.

Now you can see the meaning of my title. When asked to talk about "Property in Cyberspace," my immediate reaction was, "Isn't this just the law of the horse?" I don't know much about cyberspace; what I do know will be outdated in five years (if not five months!); and my predictions about the direction of change are worthless, making any effort to tailor the law to the subject futile. And if I did know something about computer networks, all I could do in discussing "Property in Cyberspace" would be to isolate the subject from the rest of the law of intellectual property, making the assessment weaker. . . .

Well, then, what can we do? By and large, nothing. If you don't know what is best, let people make their own arrangements.

Next after nothing is: keep doing what you have been doing. Most behavior in cyberspace is easy to classify under current property principles. . . . What else is there to do? I offer three themes.

1. Make rules clearer, to promote bargains. "We" don't know what is best, but in a Coasean world the affected parties will by their actions establish what is best.

The federal government's Working Group on Intellectual Property Rights recently issued a report called Intellectual Property and the National Information Infrastructure. In addition to the pompous title and the standard drumbeat of calls for more studies, this report contains a few concrete proposals. One, which I gather is controversial, is to amend the Copyright Act to beef up the distribution right. The Working Group recommends that the law recognize that dissemination of copyrighted works via electronic transmission is one of the rights the copyright proprietor possesses.

One may say in response that this change gives too much to the copyright proprietor or restricts unduly the ability to disseminate works. Some people believe that copyright proprietors should be delighted to have a throng willing to transmit their works to consumers who will pay royalties for them (as a recipient clearly must do — for they get a copy whether or not a transmission is a "distribution" of the work). Perhaps so; but if this is so, the author or owner will permit the transmission, just as song writers license the transmission of their works over the radio to people who may choose to turn on their tape

recorders. An author could give this permission at large, while retaining the right to charge for the keeping of copies.

Simply put, it is awfully hard to know what the optimal compensation package for authors is, unless the property rights are clear. If something about the nature of cyberspace has made application of the distribution right cloudy, then by all means clear it up again, so that people may make their own arrangements. And on balance it is best to give these rights to authors. Why? Because if the best arrangement turns out to be free distribution, then private transactions may produce this result when the statute assigns the rights to authors; but if the best arrangement turns out to be some fee for distribution and a lower price for copying, it is extremely hard to reach this state of affairs if the statute cancels the distribution right. Private transactions could shift the right back to authors only if the parties have contractual relations (for example, patrons of the opera may agree not to tape the performances). We must bear in mind the high possibility of error in the original specification of entitlements — a risk especially high in a legislative world dominated by interest-group politics. (The copy law contains a special provision for agricultural fairs and exhibitions, still another allusion to the law of the horse!) The risk of error should lead to initial assignments that are easy to reverse, so that people may find their own way with the least interference.

2. Create property rights, where now there are none — again to make bargains possible.

Property rights in domain names is an example of what I have in mind. Until recently, domain names on the Internet were assigned by the government (rather, by a firm under contract to do the government's bidding). Allocation was first-come, first-served, with no effort to purge unused names. That led to people storing up domain names. Intellectual-property law rightly has been hostile to such maneuvers. Domain names have some of the attributes of trademarks; but one can't get a trademark by just filing. A firm must use a mark to obtain rights in it; must use the mark continuously; and once this occurs, latecomers stand behind it in line. Similarly, corporate names are registered with the states, and new arrivals cannot duplicate existing names.

The allocation of domain names is now in private hands, and the $50 annual fee will abate the snatch-and-grab incentive to a limited degree. But the allocation of names remains first-come, first-served, with the result that people lay claims to famous corporate and political names. Today you can point your browser to www.clinton96.org and find, not the home page for the Clinton reelection campaign, but a satire of that campaign, with a big picture of the President holding up one finger and a caption claiming that he has a single accomplishment — election. Dick Tuck has come to cyberspace. This is nonpartisan harassment: www.dole96.org also is a satire page.

Property rights need to be better specified than that. Appropriation of names and trademarks would not be tolerated in the rest of the commercial or political world; why so for Internet addresses? In other words, we need to bring

the Internet into the world of property law. I grant that, with search facilities, you can find the American Broadcasting Corporation even if someone else has www.abc.com. Nodes are in the end numbers, and conversion to letters is arbitrary. But the search process is costly and can be avoided by correct allocation in the first place.

By "correct" allocation I certainly do not mean allocation according to some government formula. We have tried that approach with broadcast licenses, and it has failed. Indeed, even in the world of over-the-air communications, the Federal Communications Commission has moved in the direction Ronald Coase and Leo Herzel pointed in the 1950s: sell frequencies at auctions. So it can be with domain names. Let people bid for symbols, then sell them in a developed aftermarket. Perhaps initial allocations could be made by corporate names or product trademarks. Details are far less important than the principle that it is important to establish property rights, without which welfare-increasing bargains cannot occur. . . .

3. Create bargaining institutions.

Computers offer many opportunities to do, at next to no cost, the sort of thing the Copyright Clearance Center has tried and failed to do for photocopies. Consider, for example, the question whether a publisher of content on the Internet wants to authorize the making of copies and, if so, the making of copies that can be recopied, or a single copy for use on a local computer. Or does the publisher only want to authorize viewing on screen? All are logical possibilities, each rational for some authors, or for any given author at different times. How is it possible to specify which is which, and to collect payment? — especially in a world where Netscape Navigator is making cache copies behind everyone's back and turning all of you into persistent infringers!

The answer, it seems to me, is a convention — a protocol under which each file contains its own instructions on this question, and programs know how to interpret them. You are familiar with such conventions. When your modem calls a remote modem, the two devices engage in elaborate interrogation to discover what speed to use and what compression and error-correction algorithms are in place. An international standards-setting organization agreed on the language; private firms all over the world have decided whether, and to what extent, to use this agreed language for communications. Some firms have come up with their own extensions, outside the organization's framework. Encryption technology is similar. You may notice that when Netscape enters a particular corner of the web, a solid key appears in the lower left of the screen; this shows that the client and the server have agreed on an encryption protocol, securing the session.

There are several available protocols. So can it be with copying. A standards-setting organization could prescribe, say, twenty different copying rules — sets of permission and payment terms. There could be competing organizations, with their own standards. Each Internet server and client

would understand these terms and carry out the negotiation automatically, remitting any payment to an agreed depository by secure methods. . . .

A quick summary: Error in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world that we understand poorly. Let us instead do what is essential to permit the participants in this evolving world to make their own decisions. That means three things: make rules clear; create property rights where now there are none; and facilitate the formation of bargaining institutions. Then let the world of cyberspace evolve as it will, and enjoy the benefits.

Lawrence Lessig
The Law of the Horse: What Cyberlaw Might Teach

113 Harv. L. Rev. 501 (1999)

[Judge] Easterbrook's concern is a fair one. Courses in law school, Easterbrook argued, "should be limited to subjects that could illuminate the entire law." "[T]he best way to learn the law applicable to specialized endeavors," he argued, "is to study general rules." This "the law of cyberspace," conceived of as torts in cyberspace, contracts in cyberspace, property in cyberspace, etc., was not.

My claim is to the contrary. I agree that our aim should be courses that "illuminate the entire law," but unlike Easterbrook, I believe that there is an important general point that comes from thinking in particular about how law and cyberspace connect.

This general point is about the limits on law as a regulator and about the techniques for escaping those limits. This escape, both in real space and in cyberspace, comes from recognizing the collection of tools that a society has at hand for affecting constraints upon behavior. Law in its traditional sense — an order backed by a threat directed at primary behavior — is just one of these tools. The general point is that law can affect these other tools — that they constrain behavior themselves, and can function as tools of the law. The choice among tools obviously depends upon their efficacy. But importantly, the choice will also raise a question about values. By working through these examples of law interacting with cyberspace, we will throw into relief a set of general questions about law's regulation outside of cyberspace.

I do not argue that any specialized area of law would produce the same insight. I am not defending the law of the horse. My claim is specific to cyberspace. We see something when we think about the regulation of cyberspace that other areas would not show us. . . .

Many believe that cyberspace simply cannot be regulated. Behavior in cyberspace, this meme insists, is beyond government's reach. The anonymity and multi-jurisdictionality of cyberspace makes control by government in cyberspace impossible. The nature of the space makes behavior there unregulable.

This belief about cyberspace is wrong, but wrong in an interesting way. It assumes either that the nature of cyberspace is fixed — that its architecture, and the control it enables, cannot be changed — or that government cannot take steps to change this architecture.

Neither assumption is correct. Cyberspace has no nature; it has no particular architecture that cannot be changed. Its architecture is a function of its design — or, as I will describe it in the section that follows, its code. This code can change, either because it evolves in a different way, or because government or business pushes it to evolve in a particular way. And while particular versions of cyberspace do resist effective regulation, it does not follow that every version of cyberspace does so as well. Or alternatively, there are versions of cyberspace where behavior can be regulated, and the government can take steps to increase this regulability.

To see just how, we should think more broadly about the question of regulation. What does it mean to say that someone is "regulated"? How is that regulation achieved? What are its modalities? . . .

Four Modalities of Regulation in Real Space and Cyberspace

Behavior, we might say, is regulated by four kinds of constraints. Law is just one of those constraints. Law (in at least one of its aspects) orders people to behave in certain ways; it threatens punishment if they do not obey. The law tells me not to buy certain drugs, not to sell cigarettes without a license, and not to trade across international borders without first filing a customs form. It promises strict punishments if these orders are not followed. In this way, we say that law regulates.

But not only law regulates in this sense. Social norms do as well. Norms control where I can smoke; they affect how I behave with members of the opposite sex; they limit what I may wear; they influence whether I will pay my taxes. Like law, norms regulate by threatening punishment ex post. But unlike law, the punishments of norms are not centralized. Norms are enforced (if at all) by a community, not by a government. In this way, norms constrain, and therefore regulate.

Markets, too, regulate. They regulate by price. The price of gasoline limits the amount one drives — more so in Europe than in the United States. The price of subway tickets affects the use of public transportation — more so in Europe than in the United States. Of course the market is able to constrain in this manner only because of other constraints of law and social norms: property and contract law govern markets; markets operate within the domain permitted by social norms. But given these norms, and given this law, the market presents another set of constraints on individual and collective behavior.

And finally, there is a fourth feature of real space that regulates behavior — "architecture." By "architecture" I mean the physical world as we find it, even if

"as we find it" is simply how it has already been made. That a highway divides two neighborhoods limits the extent to which the neighborhoods integrate. That a town has a square, easily accessible with a diversity of shops, increases the integration of residents in that town. That Paris has large boulevards limits the ability of revolutionaries to protest. That the Constitutional Court in Germany is in Karlsruhe, while the capital is in Berlin, limits the influence of one branch of government over the other. These constraints function in a way that shapes behavior. In this way, they too regulate.

Norms regulate behavior in cyberspace as well: talk about democratic politics in the alt.knitting newsgroup, and you open yourself up to "flaming" (an angry, text-based response). "Spoof" another's identity in a "MUD" (a text-based virtual reality), and you may find yourself "toaded" (your character removed). Talk too much on a discussion list, and you are likely to wind up on a common "bozo" filter (blocking messages from you). In each case norms constrain behavior, and, as in real space, the threat of ex post (but decentralized) sanctions enforce these norms.

Markets regulate behavior in cyberspace too. Price structures often constrain access, and if they do not, then busy signals do. (America Online (AOL) learned this lesson when it shifted from an hourly to a flat-rate pricing plan.) Some sites on the web charge for access, as on-line services like AOL have for some time. Advertisers reward popular sites; on-line services drop unpopular forums. These behaviors are all a function of market constraints and market opportunity, and they all reflect the regulatory role of the market.

And finally the architecture of cyberspace, or its code, regulates behavior in cyberspace. The code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave. The substance of these constraints varies — cyberspace is not one place. But what distinguishes the architectural constraints from other constraints is how they are experienced. As with the constraints of architecture in real space — railroad tracks that divide neighborhoods, bridges that block the access of buses, constitutional courts located miles from the seat of the government — they are experienced as conditions on one's access to areas of cyberspace. The conditions, however, are different. In some places, one must enter a password before one gains access; in other places, one can enter whether identified or not. In some places, the transactions that one engages in produce traces, or "mouse droppings," that link the transactions back to the individual; in other places, this link is achieved only if the individual consents. In some places, one can elect to speak a language that only the recipient can understand (through encryption); in other places, encryption is not an option. Code sets these features; they are features selected by code writers; they constrain some behavior (for example, electronic eavesdropping) by making other behavior possible (encryption). They embed certain values, or they make the realization of certain values impossible. In this sense, these features of cyberspace also regulate, just as architecture in real space regulates.

These four constraints — both in real space and in cyberspace — operate together. For any given policy, their interaction may be cooperative, or competitive. Thus, to understand how a regulation might succeed, we must view these four modalities as acting on the same field, and understand how they interact.

Raymond Ku
Foreword: A Brave New Cyberworld?

22 T. Jefferson L. Rev. 125 (2000)

[C]yberspace is here, and it falls upon this generation to explore and understand what has been called the electronic frontier.

Equating cyberspace with an electronic frontier invokes a mythology deeply ingrained in this Nation's collective imagination and character. As Frederick Jackson Turner recognized, the frontier, as a metaphor and reality, played an important role in this Nation's early history and development. The dictionary defines frontier as "[a] region just beyond or at the edge of a settled area," or "[a]n undeveloped area or field for discovery or research." The American West and outer space clearly fit the former definition while the human genome project clearly fits the latter. With respect to the Internet, many have argued that cyberspace is in fact a region just beyond real space. According to this school of thought, the Internet is not only a place, it is many different places. As a place, it has its own rules and some have suggested should have its own sovereignty.

We are asked to accept a description of cyberspace as a world much like the one depicted in the science fiction movie The Matrix, a computer generated world where human beings interact with one another just as they do in the real world, but through the filters of technology. In the Matrix, one experiences emotions such as pain, joy, and sadness, participates in activities such as work, study, and recreation, and lives life indistinguishable from life in the real world. If you die in the Matrix, you die in the real world. In fact, the movie's premise is that human beings are tricked into believing that the computer generated virtual world is the real world. While it may be that someday we will generate virtual realities that not only have a psychic but a physical effect upon us, that day is not yet upon us.

Moreover, cyberspace is more than email, the World Wide Web or the world between the wires; it encompasses the ever-present mingling of technology in our everyday lives as well, an ever growing real world mediated by microprocessors — a cyberworld. From smart credit cards which tell stores not only whether we can make the purchase but what we have purchased in the past, to cellular telephones that allow us to reach out to anyone around the world while making it possible for others to reach us, to on-board automobile navigation systems that help us to find a friend's home and which also allow others to track our movements, to home security systems that not only sound

an alarm when someone tries to enter the home, but allow us to turn lights on and off from remote locations, we live in a world increasingly interconnected by technology. Accordingly even if cyberspace is its own place, it is also increasingly part of the cyberworld of real space. Fortunately, to appreciate its impact upon our society in general and our law in particular, it does not matter whether cyberspace should be treated as a place or not. It is not what cyberspace is (especially since cyberspace changes quicker than pundits can write), but what cyberspace and our cyberworld represent that matters.

What does the electronic frontier represent? In his seminal work, Frederick Jackson Turner described the value of the frontier in American life as much more than the addition of new territory or the exploration of a new body of knowledge. According to Turner, "[w]hat the Mediterranean Sea was to the Greeks, breaking the bond of custom, offering new experiences, calling out new institutions and activities, that and more, the ever retreating frontier has been to the United States." Like the American frontier of the 19th century, therefore, cyberspace is important because is represents an opportunity to examine and perhaps to reinvent ourselves and our society. Cyberspace presents us with an opportunity to break the bonds of existing law and customs, to create new institutions, and yes, to create new experiences.

As lawyers, judges, lawmakers, and scholars we have an obligation to examine the law and cyberspace and to take part in the discourse on how our cyberworld will be regulated. While Judge Easterbrook is clearly right that this effort requires a general understanding of the laws of intellectual property, antitrust, or the First Amendment, I disagree with his conclusion that the study of cyberspace does not "illuminate the entire law." With each inevitable controversy involving the Internet, the law is forced to confront cyberspace on two levels. On one level, we will be asked such questions as: what real space rules and legal regimes, if any, should be applied to cyberspace? Do the issues arising from cyber-conflicts fit into existing regimes or must new rules and perhaps new institutions be created to resolve these cyber-conflicts? At this level, we are asked to translate where possible our existing values and legal principles into values and principles applicable to cyberspace. While some like Judge Easterbrook may find these problems rather mundane or argue that this process of translation is not unique to cyberspace, few would consider them simple. For example, does the use of a meta-tag represent the use of a trademark? Is the process and code of one click shopping entitled to patent protection? Are Internet service providers public accommodations? Are the free speech rights of ISPs violated by regulations requiring open access? While the answer to these questions depends upon a thorough understanding of existing legal doctrine, that understanding must still be applied to a technology that many still do not comprehend and which may not fit into existing paradigms. As Judge Buckwalter recognized in American Civil Liberties Union v. Reno, in cyberspace "even commonly understood terms may have different connotations or parameters. . . ." Consequently, even skilled practitioners and legal experts may find themselves through the proverbial looking

glass when it comes to applying existing law to the new and rapidly changing cyberworld.

More importantly, pioneering our cyberworld and determining the rules and laws that will govern, forces us to examine our pre-cyberworld rules as well as our commitment to the values that form the foundation for those laws. As a new frontier, cyberspace, like the Western frontier, reopens "the debate over values that always precede the formation of principles and always infuses the effort to implement and interpret" law and legal principles. In other words, before we can coherently apply existing law to the challenges posed by cyberspace, we must resolve conflicting values and clarify the latent ambiguities that justify existing legal rules. In so doing, we may ultimately be forced to alter the laws of real space in light of our new understanding. For example, in order to resolve whether data mining violates consumer privacy, we must understand the values protected by current real space privacy laws. By the time we reach consensus on the values these laws are meant to uphold, we may ultimately conclude that the existing rules must be discarded as inconsistent with those values. Our concerns today about invasion of privacy in cyberspace, therefore, may not represent anything unique to cyberspace, but instead reflect our discomfort and concern over the loss of privacy in real space. By creating new activities and experiences, cyberspace sheds new light on old conflicts demanding their resolution. Accordingly, the resolution of these value conflicts will have an impact that extends far beyond the borders of cyberspace. As we take part in the discourse over how cyberspace should be regulated, we will ultimately come to better understand how real space should be regulated as well.

COMMENTS AND QUESTIONS

1. Is Easterbrook's assumption that lawyers do not understand technology, and, therefore, that they are "blind" trailblazers accurate? To what extent does this represent a generational gap? If it is purely a generational gap, can we expect to see this changing over time?

2. Even if Easterbrook's assumption is correct with respect to some lawyers, does it matter? Is a Nobel Prize in computer science (or economics for that matter) necessary before one can study a body of law from a multidisciplinary perspective?

3. Must every course illuminate the study of law in general? For example, to what degree does a course in property illuminate the entire law? Is property law merely a compilation of separate legal doctrines that all revolve around real property?

4. Easterbrook concludes his comments (extracted above) with the suggestion that we should not match an imperfect legal system to an evolving world that we understand poorly. The solution, in his words, is to: "make rules clear; create property rights where now there are none; and facilitate the formation of bargaining institutions." Could this approach itself be described as a

framework for a new field of law called cyberlaw or Internet law? Might a new field of law be characterized by these kinds of principles applied to cyberspace activities?

5. Do the responses provided by Lessig and Ku address Easterbrook's concerns? Do they necessarily reject Easterbrook's primary concern? Ku suggests, for example, that resolving some issues in cyberspace — such as personal privacy rights — might also illuminate related issues in the "real world." Does this suggestion confirm Easterbrook's concerns?

6. Recognizing that computer code regulates human behavior, how does that fact illuminate the entire law? For an extended discussion of Lessig's theory, see Lawrence Lessig, *Code Version 2.0* (Basic Books, 2006). See also Andrew L. Shapiro, *The Control Revolution* (Public Affairs Council for Education, 1999); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Tex. L. Rev. 553 (1998).

7. Since the above articles were written, a number of commentators have entered the debate about the nature of the Internet and cyberspace, and how/whether digital information, or digital information systems, might be effectively regulated. Some of these issues are taken up in more detail in Chapter 2. Different perspectives on these questions arise in the following articles: Alfred Yen, *Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace*, 17 Berkeley Tech. L.J. 1207 (2002); Orin Kerr, *The Problem of Perspective in Internet Law*, 91 Geo. L.J. 357 (2003); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 Cal. L. Rev. 439 (2003); Mark Lemley, *Place and Cyberspace*, 91 Cal. L. Rev. 521 (2003); Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 Loy. U. Chi. L.J. 235 (2003); Jacqueline Lipton, *A Framework for Information Law and Policy*, 82 Or. L. Rev. 695 (2003).

8. Another important development since the early days of the Internet has been the move from the early "passive" Internet to what has been described as Web 2.0. Web 2.0 is characterized by a high degree of interactivity between participants, as opposed to Web 1.0 — the early Internet — which tended to be characterized by Internet users passively receiving information posted by governments, educational institutions, businesses, and large media organizations. Examples of Web 2.0 technologies include virtual worlds like Second Life (www.secondlife.com), digital video sharing services such as YouTube (www.youtube.com), online social networking services, such as MySpace (www.myspace.com) and Facebook (www.facebook.com), and online wikis where groups of people collectively contribute information to a shared common enterprise, such as Wikipedia (www.wikipedia.org). As described by Tapscott and Williams: "The new Web is fundamentally different in both its architecture and applications. Instead of a digital newspaper, think of a shared canvas where every splash of paint contributed by one user provides a richer tapestry for the next user to modify or build on. Whether people are creating, sharing, or socializing, the new Web is principally about participating

rather than about passively receiving information." (Donald Tapscott & Anthony D. Williams, *Wikinomics: How Mass Collaboration Changes Everything*, 37 (Portfolio, 2006/2008). Does this evolution of the Internet change how we think about the early views by Easterbrook, Lessig, and Ku in relation to the nature of cyberlaw? Does Web 2.0 potentially make cyberlaw less a "law of the horse" than initially contemplated by Easterbrook? Does Web 2.0 raise the significance of the interaction between the four regulatory modalities identified by Lessig?

Note: Cyberspace and the Regulation of Information

Ever since Judge Easterbrook compared Internet law classes with teaching the Law of the Horse (in other words, Internet law has no truly distinct value aside from being one of many potential areas for applying every legal discipline from antitrust to zoning law), scholars who teach and work in this area of law have felt the need to respond to this charge. In fact, the criticism is accurate to a certain extent if the only unifying theme of a course on "Internet law" are the keywords: Internet or cyberspace.

We believe that it is a mistake to treat Internet law as a smorgasbord of controversial cases or a survey through all the areas of law that touch upon the Internet. Every area of law will eventually be forced to address Internet issues. (To provide a grand tour would entail condensing all of law into one course.) Titling this book *Cyberspace Law* is in part a linguistic attempt at separating this casebook from such an approach. More importantly, however, our use of cyberspace rather than Internet represents a shift in the substantive focus of the materials and why these courses should be taught.

Cyberspace law is inherently about the regulation, control, and dissemination of information in a world mediated by computers. The Internet is after all simply a global network of computers designed for the high-speed transmission of data within and among its constituent networks. What we generally refer to as the Internet (e-mail, the World Wide Web, newsgroups, etc.) represents only a portion of the communications enabled by this global network. The convergence of print, audio, and video programming into a single medium, the monitoring of consumer spending habits on both the Web and in real space, the ability to monitor and bill individuals for the number of times they listen to a song or operate a particular computer program, and even video surveillance linked to computers capable of face recognition to identify individuals from anywhere in the nation are other activities made possible by this global communications medium. All of these activities involve the dissemination and control of information in a networked world.

The study of cyberspace law is, therefore, the study of the regulation of information in a world interlinked and mediated by computer networks. While existing doctrines such as freedom of speech, intellectual property, and privacy are starting points, cyberspace allows and often requires a reexamination of the

values underlying those areas of law not only to translate those values into cyberspace applications, but to alter existing rules and legal institutions in real space as well. While this book is organized according to preexisting categories of information law, students should question whether those categories can and should remain discrete. In other words, the study of cyberspace law is the study of whether traditionally separate substantive laws that dealt with information should give way to a new overarching category of information law.

The study of cyberspace law is also a vehicle for exposing students to other important lessons. These include the limits of judicial and legislative responses to new technology, the malleability of computer code, the public and private regulation of behavior in the information age, and the challenges of regulating information across borders. Our goal is to provide materials that will foster lively discussion on the significant Internet cases, help students to translate existing legal rules to cyberspace, and provide materials and an organization that facilitate discourse on the larger question of information regulation.

Cyberspace and the Law of the Horse' (1996) University of Chicago Legal Foundation 207. Judge Easterbrook.Â "This is an essay about law in cyberspace. I focus on three interdependent phenomena: a set of political and legal assumptions that I call the jurisprudence of digital libertarianism, a separate but related set of beliefs about the state's supposed inability to regulate the Internet, and a preference for technological solutions to hard legal issues on-line. The Laws of Cyberspace. Lawrence Lessigâ€ Draft 3. Â©Lessig 1998: This essay was presented at the Taiwan Net â€™98 conference, in Taipei, March, 1998. â€ Jack N. and Lillian R. Berkman Professor for Entrepreneurial Legal Stud-ies, Harvard Law School. Thanks to Tim Wu for extremely helpful com-ments on an earlier draft. Lessig: The Laws of Cyberspace. Draft: April 3, 1998. Before the revolution, the Tsar in Russia had a system of in-ternal passports.