Chapter One

INTRODUCTION

The emergence of a global network of interconnected computers able to access, store, process, and transmit vast amounts of information in digital form has already altered our cultural landscape and, in the decades to come, may help to transform many of our assumptions about communication, knowledge, invention, information, sovereignty, identity, and community. Inevitably, these tremendous cultural changes bring with them new legal challenges and new legal questions, not only about how law is to be applied to a new technology, but, more fundamentally, about what law is, how it is formed, and its relation to the culture of which it is a part.

It is by now no secret that law students around the country are flocking to courses exploring these sorts of questions. Indeed, nearly every law school now offers some course touching on the Internet, and many schools provide multiple options. One reason for cyberlaw’s popularity is obvious: students see an opportunity to learn a body of law that will be necessary for them to understand as they enter legal practice in the 21st century. But another aspect of cyberlaw’s importance may not be so apparent: studying cyberspace legal issues forces us to rethink established legal doctrines that many people (professors as well as students) may have taken for granted, and to question some of the premises that underlie our thinking about the law and the way that the law operates.

Cyberlaw, in other words, is not simply a set of legal rules governing online interaction; it is a lens through which broader conceptual debates can be re-examined, challenged, and potentially reconceived. As Sherry Turkle observed in 1995, computers have become our “test objects”—metaphors through which we come to understand reality, and as a result a whole range of classic jurisprudential conundrums might fruitfully be revisited through the prism of cyberlaw.

Because nearly every area of legal activity now involves online interaction in some way, cyberlaw (if it is to be a useful field of study)

cannot simply encompass every legal case or statute that involves online interaction. We believe what is needed is an approach that will identify a set of concerns that runs throughout the various topics that Internet law can cover, a set of principles that can unify the inquiry into such diverse topics as jurisdiction, free speech, computer crime, intellectual property, and privacy, as applied to conduct on the global network.

Accordingly, this casebook has as its explicit aim the synthesis of a coherent field of study by emphasizing the broad conceptual debates that cut across the specific areas of doctrine touched by cyberspace. In addition, we will use the rise of the Internet to encourage you to reconsider various assumptions in traditional legal doctrine. We expect that this dual focus will provide broad-based and sophisticated training in Internet-related legal issues while also helping to shape cyberlaw as a coherent and useful field of study.

We begin by examining our central thesis: in what sense is cyberlaw a separate field of study? Why not simply focus on constitutional law, or civil procedure, or contracts, or administrative law, and apply the principles underlying those domains to the problems posed by online communication? What benefit might there be to thinking about so-called cyberlaw issues in an integrated way?

SECTION A. WHY CYBERLAW?

Frank H. Easterbrook,  
Cyberspace and the Law of the Horse  
1996 U. Chi. Legal F. 207

When he was dean of [the University of Chicago School of Law], Gerhard Casper was proud that the [school] 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 * * * [and] 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.

This leads directly to my principal conclusion: Develop a sound law of intellectual property, then apply it to computer networks. Problem: we do not know whether many features of existing law are optimal. Why seventeen years for patents, a lifetime plus some for copyrights, and forever for trademarks? Should these rights be strengthened or weakened? Why does copyright have the particular form it does? What sense can one make of the fuzzball factors for fair use? How can one make these rights more precise, and therefore facilitate * * * bargains? Until we have answers to these questions, we cannot issue prescriptions for applications to computer networks.

Cyberspace reduces the effective cost of copying. This continues a trend that began when Gutenberg invented movable type and gave rise to political demand for what has become copyright law. Yet how can we tackle the question whether copying has become too easy, and therefore should be met by countervailing changes, when we have not solved the problems posed by yesterday’s technology? Consider the plain-paper photocopier. People can run off scholarly articles. To what extent may researchers copy articles from increasingly expensive journals to create a stockpile for their own future endeavors? This is a question about fair use; yet the fair-use criteria are so ambulatory that no one can give a general answer. * * *

If we are so far behind in matching law to a well-understood technology such as photocopiers—if we have not even managed to create well-defined property rights so that people can adapt their own conduct to maximize total wealth—what chance do we have for a technology such as computers that is mutating faster than the virus in *The Andromeda Strain*?

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 people freely make available is freely copyable. When people attach strings, they must be respected, and the tough question when someone copies commercial software will be whether the person making copies is a direct infringer or only a contributory infringer, and whether the remedy should be civil damages or time in prison. Lower costs of copying may make violations of the law more attractive, which suggests the allocation of additional prosecutorial resources, but movement along a cost continuum does not call for change in legal substance. * * *
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)

A few years ago, at a conference on the “Law of Cyberspace” held at the University of Chicago, Judge Frank Easterbrook told the assembled listeners, a room packed with “cyberlaw” devotees, * * * that there was no more a “law of cyberspace” than there was a “Law of the Horse”; that the effort to speak as if there were such a law would just muddle rather than clarify; and that legal academics * * * should just stand aside as judges and lawyers and technologists worked through the quotidian problems that this souped-up telephone would present. “Go home,” in effect, was Judge Easterbrook’s welcome. * * *

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.

Consider two cyber-spaces, and the problems that each creates for two different social goals. Both spaces have different problems of “information”—in the first, there is not enough; in the second, too much. Both problems come from a fact about code—about the software and hardware that make each cyber-space the way it is. The central regulatory challenge in the context of cyberspace is how to make sense of this effect of code.

1. Zoning Speech.—Porn in real space is zoned from kids. Whether because of laws (banning the sale of porn to minors), or norms (telling us to shun those who do sell porn to minors), or the market (porn costs money), it is hard in real space for kids to buy porn. In the main, not everywhere; hard, not impossible. But on balance the regulations of real space have an effect. That effect keeps kids from porn.

These real-space regulations depend upon certain features in the “design” of real space. It is hard in real space to hide that you are a kid. Age in real space is a self-authenticating fact. Sure—a kid may try to disguise that he is a kid; he may don a mustache or walk on stilts. But costumes are expensive, and not terribly effective. And it is hard to walk on stilts. Ordinarily a kid transmits that he is a kid; ordinarily, the seller of porn knows a kid is a kid, and so the seller of porn, either because of laws or norms, can at least identify underage customers. Self-authentication makes zoning in real space easy.

In cyberspace, age is not similarly self-authenticating. Even if the same laws and norms did apply in cyberspace, and even if the constraints of the market were the same (as they are not), any effort to zone porn in cyberspace would face a very difficult problem. Age is extremely hard to certify. To a website accepting traffic, all requests are equal. There is no simple way for a website to distinguish adults from kids, and, likewise, no easy way for an adult to establish that he is an adult. This feature of the space makes zoning speech there costly—so costly, the Supreme Court concluded in Reno v. ACLU that the Constitution may prohibit it.

2. Protected Privacy.—If you walked into a store, and the guard at the store recorded your name; if cameras tracked your every step, noting what items you looked at and what items you ignored; if an employee followed you around, calculating the time you spent in any given aisle; if before you could purchase an item you selected, the cashier demanded that you reveal who you were—if any or all of these things happened in real space, you would notice. You would notice and could then make a choice about whether you wanted to shop in such a store. Perhaps the vain enjoy the attention; perhaps the thrifty are attracted by the resulting lower prices. They might have no problem with this data collection regime. But at least
you would know. Whatever the reason, whatever the consequent choice, you would know enough in real space to know to make a choice.

In cyberspace, you would not. You would not notice such monitoring because such tracking in cyberspace is not similarly visible. * * * When you enter a store in cyberspace, the store can record who you are; click monitors (watching what you choose with your mouse) will track where you browse, how long you view a particular page; an “employee” (if only a bot) can follow you around, and when you make a purchase, it can record who you are and from where you came. All this happens in cyberspace—invisibly. Data is collected, but without your knowledge. Thus you cannot (at least not as easily) choose whether you will participate in or consent to this surveillance. In cyberspace, surveillance is not self-authenticating. Nothing reveals whether you are being watched, so there is no real basis upon which to consent.

These examples mirror each other, and present a common pattern. In each, some bit of data is missing, which means that in each, some end cannot be pursued. In the first case, that end is collective (zoning porn); in the second, it is individual (choosing privacy). But in both, it is a feature of cyberspace that interferes with the particular end. And hence in both, law faces a choice—whether to regulate to change this architectural feature, or to leave cyberspace alone and disable this collective or individual goal. Should the law change in response to these differences? Or should the law try to change the features of cyberspace, to make them conform to the law? And if the latter, then what constraints should there be on the law’s effort to change cyberspace’s “nature”? What principles should govern the law’s mucking about with this space? Or, again, how should law regulate? * * *

To many this question will seem very odd. Many believe that cyberspace simply cannot be regulated. * * * 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 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? * * *
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.

These four modalities regulate together. The “net regulation” of any particular policy is the sum of the regulatory effects of the four modalities together. A policy trades off among these four regulatory tools. It selects its tool depending upon what works best.

So understood, this model describes the regulation of cyberspace as well. There, too, we can describe four modalities of constraint.

Law regulates behavior in cyberspace—copyright, defamation, and obscenity law all continue to threaten ex post sanctions for violations. How efficiently law regulates behavior in cyberspace is a separate question—in some cases it does so more efficiently, in others not. Better or not, law continues to threaten an expected return. Legislatures enact, prosecutors threaten, courts convict.
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 “toadied” (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. Prices 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.

The two problems from the beginning of this section are a simple example of this point:
(a) Zoning Speech.—If there is a problem zoning speech in cyberspace, it is a problem traceable (at least in part) to a difference in the architecture of that place. In real space, age is (relatively) self-authenticating. In cyberspace, it is not. The basic architecture of cyberspace permits users’ attributes to remain invisible. So norms, or laws, that turn upon a consumer’s age are more difficult to enforce in cyberspace. Law and norms are disabled by this different architecture.

(b) Protecting Privacy.—A similar story can be told about the “problem” of privacy in cyberspace. Real-space architecture makes surveillance generally self-authenticating. Ordinarily, we can notice if we are being followed, or if data from an identity card is being collected. Knowing this enables us to decline giving information if we do not want that information known. Thus, real space interferes with non-consensual collection of data. Hiding that one is spying is relatively hard.

The architecture of cyberspace does not similarly flush out the spy. We wander through cyberspace, unaware of the technologies that gather and track our behavior. We cannot function in life if we assume that everywhere we go such information is collected. Collection practices differ, depending on the site and its objectives. To consent to being tracked, we must know that data is being collected. But the architecture disables (relative to real space) our ability to know when we are being monitored, and to take steps to limit that monitoring.

I noted earlier the general perception that cyberspace was unregulable—that its nature made it so and that this nature was fixed. I argued that whether cyberspace can be regulated is not a function of Nature. It depends, instead, upon its architecture, or its code. Its regulability, that is, is a function of its design. There are designs where behavior within the Net is beyond government’s reach; and there are designs where behavior within the Net is fully within government’s reach. My claim is that government can take steps to alter the Internet’s design. It can take steps, that is, to affect the regulability of the Internet.

Regulability depends upon the architecture of the space, and this architecture can be changed. The code of cyberspace might disable government choice, but the code can disable individual choice as well. There is no natural and general alignment between bottom-up regulation and the existing architecture of the Internet. Enabling individual choice may require collective modification of the architecture of cyberspace, just as enabling collective choice may require modification of this architecture. The architecture of cyberspace is neutral; it can enable or disable either kind of choice. The choice about which to enable, however, is not in any sense neutral.

Architectures of cyberspace can enable or disable the values implicit in law; law, acting on architectures in cyberspace, can enable or disable the values implicit in code. As one displaces the other, a competition could
develop. Authors of code might develop code that displaces law; authors of law might respond with law that displaces code.

East Coast Code (written in Washington, published in the U.S. Code) can thus compete with West Coast Code (written in Silicon Valley, or Redmond, published in bits burned in plastic). Likewise authors of East Coast Code can cooperate with authors of West Coast Code. It is not clear which code one should fear more. The conflict displaces values in both spheres, but cooperation threatens values as well. * * *

This conflict between code and law should push us to consider principle. We should think again about the values that should guide, or constrain, this conflict between authorities. * * * Cyberspace is not inherently unregulable; * * * its regulability is a function of its design. Some designs make behavior more refutable; others make behavior less regulable. Government * * * can influence the design of cyberspace in ways that enhance government’s ability to regulate. * * *

Judge Easterbrook argued that there was no reason to teach the “law of cyberspace,” any more than there was reason to teach the “law of the horse,” because neither, he suggested, would “illuminate the entire law.” This essay has been a respectful disagreement. The threats to values implicit in the law—threats raised by changes in the architecture of code—are just particular examples of a more general point: that more than law alone enables legal values, and law alone cannot guarantee them. If our objective is a world constituted by these values, then it is as much these other regulators—code, but also norms and the market—that must be addressed. Cyberspace makes plain not just how this interaction takes place, but also the urgency of understanding how to affect it.

Notes and Questions

1. Why does Judge Easterbrook believe that cyberlaw is not a distinct field of study? Why does he think courses in torts or property are more appropriate?

2. Judge Easterbrook argues that law does a poor job adjusting to changes in technology. While it is certainly true that such changes often raise difficult questions, what is the appropriate response for judges and legislators? Should they get out of the way, as Judge Easterbrook suggests, and “let the world of cyberspace evolve as it will”? What are the consequences of such a choice? Are the consequences different in cyberspace than in other areas of law?

3. Why didn’t the University of Chicago Law School offer a course in the “Law of the Horse,” anyway? Thirty or forty years ago, few law schools recognized “family law,” or “elder law,” or “environmental law” as valid subfields worthy of study, yet most do now. Is “cyberspace law” more like family law or the “law of the horse”?

4. What does Lessig mean when he talks of “East Coast Code” and “West Coast Code”? What is the relationship between “code” and law?

5. Think about the two examples cited by Lessig: controlling indecent material and protecting privacy. How might altering “code” affect these
problems in the online environment? What might Judge Easterbrook think of using code to “solve” online problems?

6. What role should government play in influencing the “code” of cyberspace? What role can it play? Lessig declares his disagreement with those who believe that cyberspace cannot be regulated by territorial sovereign governments; we will explore these questions when we discuss problems of geography and sovereignty in Chapter Three.

7. In what ways might cyberspace not only permit us to revisit problems of jurisprudence, but also cause us to change our concepts of self and community? Consider the following excerpt:

Writing in his diary in 1832, Ralph Waldo Emerson reflected that “Dreams and beasts are two keys by which we are to find out the secrets of our nature . . . they are our test objects.” Emerson was prescient. Freud and his heirs would insist that we measure human nature against nature itself—the world of the beasts seen as our forbears and kin. If Emerson had lived at the end of the twentieth century, he would surely have seen the computer as a new test object. Like dreams and beasts, the computer stands on the margins. It is a mind that is not yet a mind. It is inanimate yet interactive. It does not think, yet neither is it external to thought. It is an object, ultimately a mechanism, but it behaves, interacts, and seems in a certain sense to know. It confronts us with an uneasy sense of kinship. After all, we too behave, interact, and seem to know, and yet are ultimately made of matter and programmed DNA. We think we can think. But can it think? Could it have the capacity to feel? Could it ever be said to be alive? * * * The computer is an evocative object that causes old boundaries to be renegotiated.


What does Professor Turkle mean when she refers to computers as “test objects”? Can you think of ways in which the pervasiveness of the computer, the common reference to virtual realities such as “desktops” or “folders” on a screen, and the use of various forms of online interaction (e-mail, web-based communities, hypertext linking, multi-player games and virtual worlds, etc.) might change the way we think of ourselves and the world? For example, if we become used to interacting with simulated objects and with manipulating multiple screens at once, does that change our conceptions of what makes something “real,” or what distinguishes human beings from computers, or what makes a self coherent? If we are used to linking from one website to another, picking and choosing bits of information to read, does that change our sense of whether ideas are linear or whether individual authorship is possible, or whether ownership of intellectual property is sensible? If we daily interact by e-mail or in virtual communities, does that change our conception of distance or the importance of territorial boundaries or geographically based communities? Can you think of any other long-term cultural effects of the information age that might usefully be viewed through the lens of cyberlaw?
SECTION B. OUR APPROACH

We believe that cyberspace presents us with an opportunity to view general problems of policy, jurisprudence, and culture in a new and useful way. We will not, therefore, approach online legal issues along traditional doctrinal lines—First Amendment, jurisdiction, copyright, contracts, and so on—for to do so would presuppose precisely what we intend to question: that traditional doctrinal approaches map neatly and simply onto online phenomena. Instead, we have organized the material that follows according to a set of conceptual issues that extends across the spectrum of cyberspace legal dilemmas. This approach is meant both to illuminate the legal conundrums posed by online activity and to encourage you to explore more general topics such as: the role of analogy in developing legal rules for new social contexts such as the rise of cyberspace; the difficulties territorially based sovereign entities face in attempting to regulate any online activity, whether it involves gambling, or the transmission of sexually explicit material, or the distribution of copyrighted material, or the like; the possibility of alternative models of Internet governance; the ways in which law and technological architecture conflict with, or reinforce, each other as regulatory tools; the role played by the competing rhetorics of anarchy and control in debates about online regulation; the rise of so-called “private ordering” approaches to the creation of law and social norms; the complicated position of “intermediaries” (such as Internet service providers) within regulatory regimes, and many others. While all of the “traditional” subject matter areas of cyberlaw will be addressed, they will be placed in a new framework—one that asks you to consider what it is that cyberlaw has to teach us about law more generally.

In addition, this casebook will focus on the way legal and cultural norms interact and shape one another. Most casebooks study the role of law solely as a mechanism for resolving disputes, or meting out punishment, or creating incentives, or regulating behavior. This view emphasizes the instrumental role of law; that is, the role of law as a rational effort to do something to affect society. But that is not all there is to law. Law is also a discourse for conceptualizing reality, or, as anthropologist Clifford Geertz put it, a way of “imagining the real,” a mechanism through which we construct meaning from the world around us. It is a “complex of characterizations and imaginings, stories about events cast in imagery about principles.” These stories provide a framework to interpret what we experience and a language for describing reality.

Because law does not exist in a vacuum, any particular cyberlaw regime will inevitably have tremendous impact on the distribution of power in society as a whole, our understanding of terms such as free speech,


c. Id. at 215.
intellectual property, and jurisdiction, as well as our fundamental conceptions of how behavior is regulated both online and off. Thus, this casebook will provide not simply an introduction to legal issues involving online interaction, but a chance to consider and challenge core ideas about the role of law more generally. Finally, because we must try to understand the cultural significance of cyberspace in all its variety before we impose any single legal category on the experience of being “online,” we will devote a chapter to the psychological, social, and political ramifications of cyberspace.

In order to structure your thinking, you may wish to consider five fundamental questions that will recur throughout the book:

- Does the rise of a global network present a new paradigm that requires a completely different way of thinking about law, or is it just a matter of adapting current legal categories to new technology?
- Is it best to allow law in cyberspace to evolve internally, through indigenous legal regimes, or must a uniform regime be imposed from outside? And is it even possible for cyberspace to have an “internal” legal regime totally divorced from more traditional “outside” legal systems?
- To what extent will regulation in cyberspace be accomplished through its technical architecture, and to what extent does this form of regulation affect how we develop policy on cyberspace issues?
- In what ways does the rise of online interaction alter the balance of power among individuals, corporations, and government, and how should our choice of legal regime be influenced by these changes?
- How does thinking about cyberspace legal issues help illuminate more general issues of policy and jurisprudence?

SECTION C. INTERNET BASICS

Professor Lessig suggests that “technical” questions and “legal” questions—questions about “code” and questions about “law”—will interact in complex ways, and may often substantially overlap, in cyberspace. While one does not have to be a systems engineer to understand and analyze the legal issues posed by online interaction, some understanding of the underlying technologies will be useful; even Judge Easterbrook, we suspect, would agree that one has to know something about how cyberspace is constituted in order to apply the “general principles” to which he refers in the online context, just as a knowledge of horse behavior or anatomy would be useful in order to apply the general principle, say, of “reasonable care” to the horse owner.
The Internet, as most people know by now, is not a physical entity but rather a network of networks—an inter-network, a set of communications links and communications rules (known as “protocols”) allowing computer networks to exchange information with one another. It is only one of many thousands of such inter-networks out there; numerous businesses, for example, operate private inter-networks linking their remote office or retail locations together. The Internet had its origins in 1969 as an experimental networking project supported and managed by the Advanced Research Project Agency (“ARPA”) of the U.S. Department of Defense. Known then as the “ARPANET,” it linked together computers and computer networks owned by the military, defense contractors, and university laboratories conducting defense-related research. On January 1, 1983, the networks comprising the ARPANET—then numbering under one thousand—switched over to the TCP/IP protocol suite (“Transmission Control Protocol/Internet Protocol”) to manage network communications, and the network that was to become “the Internet” was born. By 2006, the TCP/IP network had over 400 million individual “hosts”—computers, or computer networks, capable of exchanging messages with one another.

What made the TCP/IP inter-network so successful? Why did this particular set of networking protocols spawn “the Internet,” i.e., the vast, global communications medium? “Much of the answer,” the National Research Council wrote in a recent study,

lies in the combination of two factors: functionality and lower costs. The new functionality stems from the Internet’s unique design principles and features that make connection, interconnection, and innovation in both facilities and services relatively easy. The Internet’s characteristics have also made it possible to use the underlying communications infrastructure more efficiently, thereby setting a lower price point for the communications it enables.


Although the technical architecture of the Internet is always subject to change, it is worth reflecting on what aspects of the Internet’s design have made it particularly useful as a communications medium. Such “unique design principles and features” may or may not be considered part of the Internet’s “nature,” but to the extent that we acknowledge how successful the Internet has been, we might at least want to think twice before disabling fundamental features about the Internet that have fueled its growth. Some of those design features are:

A. Decentralized Control. Unlike many other networks (most office LANs and university networks, for instance), TCP/IP networks like the Internet have no central “server” responsible for managing network traffic
and seeing to it that messages reach their intended destinations. Instead, messages make their way from one network host to another by traversing the network one “hop” at a time:

A message from Network A—say, in Austin, Texas—can thus take any one of a large number of alternate paths to reach its destination at Network P (Paris, France); it might travel via routers in Atlanta, Philadelphia, Newfoundland, and Stockholm before reaching its destination, or, alternatively, if that path were for some reason unavailable, via Chicago, Denver, Mexico City, Mumbai, and Brussels. This feature—known to the engineers as redundancy—allows the Internet to continue to function notwithstanding damage to, or failure by, a portion of the network; messages can be routed around the damaged portion and through alternate paths. By contrast, with more centralized designs, damage to the central server renders the entire network inoperable. This was one of the features that first appealed to the Department of Defense, because it seemed to insure the survivability of the inter-network in the face of attack.

No single entity—academic, corporate, governmental, or non-profit—administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.


B. Openness. The Internet is an “open” network in several senses. First, the TCP/IP protocols themselves, which are required in order to send and to
receive messages over the Internet, are publicly-accessible and non-proprietary (see the collection of “Internet Standards” at http://www.ietf.org); this has allowed hardware and software providers to implement the required standards relatively easily. Second, the Internet is “open” in the sense that it is easy to join; with no central server that must be informed of a new network participant, in order to communicate with others over the Internet one need only obtain the necessary software and arrange for a connection to any one of the thousands of Internet service providers worldwide. Third, the Internet is open in the sense that it can inter-connect networks that may themselves use different operating systems and underlying technologies.

C. Packet-switching. The Internet is a “packet-switched” network (as contrasted with circuit-switched networks such as the telephone network). Packet-switching means that before being transmitted over the inter-network, a message is broken up into small, fixed-length blocks (or “packets”), and each of the packets is then routed independently of the others to the recipient machine. That recipient machine is then responsible for re-assembling all of the packets—which are likely to arrive out of order, given the different routes they have taken—back into a single message. As a consequence, the physical communications lines connecting any two users on the Internet can be performing that same task for thousands, or hundreds of thousands, of users more-or-less simultaneously, as packet follows packet follows packet across the wires. By contrast, a circuit-switched network—like the telephone network—identifies a single line between sender and recipient and keeps that line “open,” dedicated exclusively to that one connection, until the communication between the two is completed. Packet-switching not only makes it more difficult to intercept and interpret messages traveling over the network (because messages have been disassembled before transmission)—another feature of the Internet’s design that appealed to military planners—it allows for a much more efficient use of available transmission capacity, allowing many more communications between many more users to travel over the same physical facilities, compared to circuit-switched networks.

D. Digital Information. The inter-network transmits information only in digital form, as on-off pulses of electrical energy representing the binary digits “1” and “0”. Physical distance is thus largely irrelevant to online communications; digital information can move nearly as quickly across the globe as across town, with no significant degradation in quality. From a technical perspective, there is no music, or pornography, or message boards, or virtual worlds, or books for sale, etc. on the Internet; there are only massive strings of 1s and 0s. And because digital information can be copied instantly and (virtually) without error (compared to analog information), copying is an essential part of the architecture itself. For example, messages are reproduced each time they move from one router to another across the network. Similarly, every time one accesses a website, a copy of the requested page is produced on one’s own computer.

E. Layered Architecture. Professor Tim Wu offers this helpful analogy to describe the Internet’s “layered” design:
What it means for a network to have a layered architecture, viewed all at once, can be at first difficult to grasp, yet the idea is so clever that it merits understanding. A network communication between computers is a very complex operation. The essence of network layering is a grand simplification by delegation to functional submodules, the layers. Dividing one large task among several layers has numerous advantages—it allows specialized efficiency, organizational coherency, and future flexibility—and is something we constantly see in the real world yet consider unremarkable.

Consider, as a way to understand this, what happens when one lawyer uses the postal system to mail a legal argument to another lawyer. The postal system is structured so that no one in the postal system needs to understand law (the language of the lawyers) for the message to be successfully delivered. And, similarly, neither lawyer need do anything more than understand the rules on addressing and postage. This makes for a simple two-layer network. The function of understanding the contents of the letter has been delegated to a “higher” layer (in this case lawyers), and the function of delivering the letter has been delegated to a “lower” layer (the postal system).

In this example, the postal level is called “lower” because it can be seen as more fundamental. The lawyers need the postal system or they cannot communicate at all; yet if the lawyers did not exist, the postal system would continue to carry mail for doctors, scientists and other interpreters of strange lingo. Notice also that the postal system is more fundamental in the sense that it can set standards that apply to everyone in the higher levels, regardless of who they are. For example, the postal service could require that all envelopes be blue. The higher-level users of the system would have no choice but to comply.

Notice several things about a network so structured. First, it allows an efficient specialization: That the postal system need not understand law (or the content of any of the messages it carries) dramatically reduces the burden on the post office and allows it to focus on one task: delivering mail. Second, the system is very flexible: The postal system can carry any type of message, and the communication will be successful, provided that the person on the other side understands it. This makes the postal system useful for a wide variety of applications. Finally, the layers are modular: Were the postal system to begin using spaceships to deliver its mail, the lawyers would be unaffected so long as the rules for postage and writing addresses remained the same.


The Internet shares this same basic layered structure—though with four, rather than two, layers.
To see roughly how Internet layering operates, suppose that you are sitting in a law school classroom, connected via a fiber optic cable to your school’s local area network and, through that connection, to the Internet, and you have just sent a request for a web page located at http://www.aclu.org. The protocols used at the physical layer determine how the electrical transmissions produced by your computer are to be converted into bit strings by the LAN server; most (but by no means all) LANs use the Ethernet protocol suite for this task. (This layer is absent from the postal system Professor Wu describes above—although one might perhaps think of the rules governing the conversion of otherwise meaningless blotsches of ink on paper into meaningful “letters” as operating at the equivalent of the “physical layer” of the postal system.)

The protocol at the network layer is the direct analogue of the postal service layer in Professor Wu’s example; it determines how the bit-strings that you have sent to your LAN server are to be addressed so that they can be routed over the inter-network to the correct recipient (“www.aclu.org”). On the Internet, the Internet Protocol is used for these tasks.

As mentioned above, the Internet Protocol requires that all messages (including your file request to www.aclu.org) be broken up into fixed-length packets before transmission over the Internet. Protocols at the transport layer govern the way in which messages are re-assembled when delivered to the recipient machines. Many different transport layer protocols are used for Internet communication, although TCP (“Transmission Control Protocol”) is the most common. Typically, transport layer protocols provide for error-correction and quality control (i.e., some way for the recipient machine to know that all of the packets comprising a single message have arrived, to check for transmission errors, and to request re-transmission of missing or damaged packets). (There is no equivalent of the transport layer in the postal system; we would need a transport layer, and a transport layer protocol, if the postal service required, for example, that all letters had to be torn up into one-inch square fragments before they could be delivered.)

Finally, there is the application layer. Just as lawyers in Professor Wu’s example use the rules of English (or, perhaps, that strange dialect known as “legalese”) to interpret and to give meaning to the messages that the postal service delivers, so, too, the recipient of your message has to decode and interpret it—to determine whether it is a request for a copy of a particular file residing on the recipient’s computer, or an e-mail message, or a voice communication, or something else. The communication you sent to www.aclu.org—having been converted into a bit-string by some physical

<table>
<thead>
<tr>
<th>Postal System Layers</th>
<th>Internet Layers</th>
</tr>
</thead>
<tbody>
<tr>
<td>User layer [rules for interpreting delivered mail]</td>
<td>Application</td>
</tr>
<tr>
<td>Postal Service [addressing rules]</td>
<td>Transport</td>
</tr>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Physical</td>
</tr>
</tbody>
</table>
layer protocol (e.g., Ethernet), broken up into packets and addressed using a network protocol (IP), transmitted to and re-assembled by the recipient machine (TCP)—uses HTTP (the “hypertext transfer protocol”) as the application layer protocol; this tells the recipient machine that this is indeed a request for the transmission of a copy of the file “Index.html” residing on the machine at the www.aclu.org address.

This architecture, as in the postal system example, allows specialization at each layer of the protocol stack; protocols at each layer operate independently of the protocols in the other layers. The network layer protocols can be designed to route packets from one place to another as quickly and as efficiently as possible, without having to know anything about what the bit-strings that are being routed “mean.” Similarly, applications can interpret the data they send to each other without worrying about how it got there—just as plumbers, doctors, lawyers, chemists, and insurance salesmen can develop and all use their own specialized lingoes for communication, secure in the knowledge the postal service will deliver their letters correctly.

F. End-to-End Design. The end-to-end design principle is closely linked to the principle of layered architecture; it holds that, wherever possible, functions should be placed at the higher layers of the protocol stack, i.e., that as much as possible should be left to software running in the applications layer—at the user “end” rather than in the network “center.” The lower-level protocols are kept as simple and unobtrusive as possible, focused only on the minimal function of transmitting data. End-to-end design means that the physical, network, and transport layer protocols will deliver a network user’s bits wherever directed—what happens to them after that point is of no concern to the network itself but is controlled entirely by the applications running on the user’s machine.

So while the basic network protocol (IP), for example, could do much more than just addressing and routing—checking for malicious code, for instance, or more aggressive security and authentication of sender identity, or any number of other functions—end-to-end leaves these functions for users to implement if they wish (or not).

End-to-end design has profound implications for the Internet’s growth and utilization. It grants the maximum possible autonomy to applications running “on top” of the basic network protocols themselves, giving application-writers the freedom to achieve their goals in whatever manner they see fit, and to innovate whenever and however they like. Virtually all of the network’s “intelligence”—the processing required to interpret the bit-strings delivered over the Internet by the lower level protocols—is located in the software running in the applications layer. Bits are bits; the network will move them around for you as directed no matter what they mean, or what they are intended to do when they reach their destination. Innovation comes in the form of new applications—e-mail, or instant messaging, or the World Wide Web, or VoIP (Voice over Internet Protocol), or peer-to-peer file-sharing—developed and deployed at the edges of the network, not the
center; the center need not participate in (nor even have any information about) those new applications. At the same time, by confining the lower level protocols to simple functions, the design avoids blocking out future applications that may be unknown and unpredictable at the time of design.

This is, again, in stark contrast to the telephone network, which was designed to allow very simple devices at the edges—telephones—to connect to a very sophisticated central processing core:

Its relatively rapid responsiveness to users and other design attributes distinguish the Internet from other parts of the information infrastructure, such as the *telephone network* or the television networks (cable and broadcast). The design of those other networks is more focused on the center, and greater functionality is located within the networks. They have been more centrally developed and managed and historically have limited what users can do with them. In contrast, the Internet’s design is effectively neutral to what services operate across the network. This enables a relatively unrestricted set of applications to run over it without the need for changes to be made within the network.
