picture the Soviet Union during its final days. Think about the most powerful within that system. These were not inherently evil people, though no doubt, especially during the Stalinist era, there were plenty of psychopaths hanging about. They were quite ordinary in many ways; if you met them at a party, many would strike you as quite liberal and sensible. They were not terribly rich, though some were. And they didn’t live in a flourishing society, though they were promised just this as they grew up in the USSR. But by the late 1980s, everyone knew the system had failed. Yet very few were willing to take steps to free that society from state control.

Why? Why wouldn’t these “leaders” try to move their society to a better place? Why wouldn’t they voluntarily push for a different system of control?

It doesn’t take a deep understanding of human psychology to answer this question. Things may have been bad, but how would these leaders know that for them and their families, things would be better under any other system? What incentive was there to release the reins of control, when the resulting system could promise so little that was certain? Like the management of a successful company, they could see the marginal improvements that were possible if they stayed on course. But they could not be confident of improvement if they jumped the other way.

(Here the story of the malevolent giant begins to make more sense. One could well believe the leaders of the Soviet Union expected their society as a whole would be better off under freedom but also believed they would not be able to extract enough of that social gain to make them individually as well off.)
Now picture the leaders of dominant industries, faced with a disruptive technology. What is their rational response? Is it any different?

The perfect marketeers presume these actors would behave differently from the Soviets. They presume the leaders of dinosaur firms would spin those firms on a dime, to become something radically different.

But why would one believe that? Faced with a disruptive technology that threatens their way of life—their mode of doing business, their vision of the market—why would these leaders voluntarily step down from their place and enter a different market with uncertain returns? Why instead isn’t the story that Christensen tells—like all deep truth—obvious, once we see it?

And even more obvious, why wouldn’t we expect these leaders of existing dominant industries to use whatever power they have to protect themselves? Rather than yielding to the new technology, wouldn’t they take steps to protect the old against the new?

What steps would these be? In the story I have told, there are any number of levers that the old Soviets might use. Most obviously, they could use the force of law to stifle innovation that challenges their power. Or they could use market power to chill the willingness of innovators to challenge their position. Or they could use norms to stigmatize the deviants. Or they could use architecture to hinder the opportunity for innovators to innovate. Any one of these techniques could help strengthen the power of the existing Soviets; any one could be deployed to weaken the opportunity of a challenger.

The balance of this book is a story about how our “old Soviets” are doing precisely this with the Internet. “Soviets” is an unfair term, I know, but the image is precise even if unfair. Changes threaten the power of those now in power; they will work in turn to protect themselves from the changes. In the balance of this book, I want to detail their work to change the Internet, and the legal culture surrounding it, to better protect themselves. Some of these changes are legal; some are technical; and some use the power of the market. But all are driven by the desire to assure that this revolution doesn’t muck things up—for them.

There’s nothing immoral in this desire. This is not a battle between good and evil. Stockholders demand that management maximize its income; we shouldn’t expect management to do anything different.

But even if this is “only business” to them, that does not mean it should be “just business” for us. We need not stand by idly as the Internet is changed. They have their interests; we have ours. And for those who believe that the environment of creativity that the Internet produced was worth something, there is reason to resist the changes that I will describe.
In Chapter 3, I described an architectural principle that I said helped build an innovation commons: end-to-end. I also described the struggle to assure that in effect that principle would govern on the telephone lines. Keeping those channels open to enable this commons of innovation was an important, if forgotten, part of the history that gave us the Internet.

The lesson from that story was of the power that came from an inability to control: the innovation and creativity that were inspired by a platform that was free.

If there was a time in the past decade when we had learned this lesson, the story of this chapter is that we have now forgotten it. The changes that I will describe in the pages that follow are all examples of the network being rearchitected for control. I have called the inability to discriminate a feature of the original Net's design. But to many—and especially those building out what the network called the Internet will become—this “feature” is a bug. The power to discriminate is increasingly the norm; building a Net to enable it is the aim.

The Internet was born on networks linking universities, but it took its first step when it came to the phones. It was when ordinary individuals could dial up an Internet connection that the Internet came alive.

Long before people started dialing into the Internet, however, many were already members of on-line services and on-line communities. CompuServe and Prodigy were early market players. America Online came a bit
later. These services were born serving content of their own. They were not Internet portals. There was indeed no way to move from their proprietary system to the nonproprietary Internet.

By the mid-1990s, all this changed as the attraction of the Internet grew, and as the competitive threat of ISPs increased. As more and more saw the Internet as an attractive alternative to the edited content of the existing service providers, they pressed their service providers to provide access to the Internet.

As I've suggested, the part of this story that is too often missed is the role that the telephone company played in the birth of the Net or, more accurately, the role the telephone company did not play. For what is striking about the birth of this different mode of communication is how little the telephone companies did in response. As their wires were being used for this new and different purpose, they did not balk. They instead stood by as the Internet was served across their wires.

This was no slight change. When telephones are used for talking, the average usage at a particular house is quite small. Calls are ordinarily short, so the number of circuits needed in a particular region is few.

But when phones began to be used to link to the Internet, this usage changed dramatically. Calls no longer lasted a few minutes on average. People were dialing in and hanging on, and the burden placed on the telephone system was great. The average voice call typically lasts only three to five minutes; the average Internet “call” lasts seventeen to twenty minutes.1

Ordinarily, one imagines that telephone companies would be quick to respond to this change in usage. They would either be quick to increase rates for calls over a certain length or they might restrict usage to certain kinds of telephone numbers (such as those to the ISPs). And we might imagine that telephone companies, if they were creative, would decide to become their own Internet service providers, offering better rates internally than they did to other Internet service providers. In short, there are any number of games telephone companies might play to respond to this demand for Internet services.

Phone companies, however, did not play these games, because they were not allowed to. And they were not allowed to because regulators stopped them.2

As we saw in chapter 3, the telephone company had become a disfavored monopoly. Its power over its wires had first been limited in 1968, in the Carterfone decision,3 and then after growing resistance by Congress and the FCC, most dramatically by the Justice Department in the early 1980s. In
1984, a decree breaking up AT&T was entered, and over the next ten years, Congress and the FCC struggled to find a model under which the Bells created by the breakup would be regulated.

The model finally fixed upon—and ratified by a statute of Congress in 1996—imposed an obligation on the Baby Bells to be neutral about how their lines would be used. The Baby Bells were required to unbundle the services they offered and make it possible for others to compete directly with them. If you wanted to start an ISP, you could connect your service into the telephone company’s office. Their wires in a sense became your wires. The important point was preserving and defending neutrality.4

This imposed neutrality had an unintended effect on the Internet and its growth, because while the regulators imagined creating competition in the telephone service, they did not have in their head the idea that this might create a kind of competition with telephone service. They did not imagine the birth of the Internet as a product of their accidental regulation. But that is precisely what their regulation produced. This imposed neutrality about how the wires would be used left the field open for others to use the wires in ways no one ever expected. The Internet was one such way.

THE END-TO-END IN TELEPHONES

As I described in chapter 3, the end-to-end argument says intelligence in a network should be located at the edge, or ends, of the network, and that the network itself should remain simple. Only those functions that must be placed in the network are placed in the network. Other functions—other intelligence—are left to the applications that run on the network.

The TCP/IP Internet was designed as an end-to-end network. The protocols of TCP/IP simply enable data to be sent across the network. They regulate how data is to be divided and how the resulting packets are shipped. They don’t at all care about what is built into the data or how that built-in part works.

Not all networks are end-to-end in this sense. A contrasting network design is, for example, an asynchronous transfer mode (ATM) design. Under the ATM design, the network first establishes a virtual circuit between two endpoints in the network; it then ships data along that circuit. The virtual circuit means the network can control quality of service. But the virtual circuit also means the network is more “intelligent” than another network.5 The circuit could be programmed to be compliant with the end-to-end
character of the original network design. But it need not be; it can be much more (intelligent) and hence much less.

These differences make it sound as if there is a fairly technical way to describe whether a network complies with “end-to-end” principles. They suggest that the question of whether a network is end-to-end is simply a question to be answered by technologists.

But let’s step back from the technical aspects and look more broadly at the types of control there might be over a network. For if value comes from the absence of control architected into a network, then that value may be compromised by other techniques of control.6

The point should be obvious, but it bears emphasis. In principle, a network could be architected such that each application must “register” itself with the network before that application will run on the network. A program would then send a request to the network—“May I run X?”—and the network would give it a digital token as permission to run. Such a network would not comply with the end-to-end argument. It would be a control-centered network that requires permission before computer resources are used. The permission this network would require is negotiated technically. The machine does the negotiating, and if you don’t get a token, your code doesn’t run.

Notice, however, that the very same control could be implemented through other means. The network, for example, could have a rule—imposed through contract—that before your computer ran any program, you would have to register that program with the network administrator. This rule would not be enforced through code—you could cheat and sometimes get away with it. But you might expect the network administrator to have code to detect whether you are cheating. And if it finds that you are cheating, it might force you off the network.

Or we might imagine a community network, where there is an understanding about the kinds of applications that would be run on the network and the kinds of applications that would not be run. Roommates might have a network, and to keep it running fast, they might have an understanding not to use the network to download MP3s. Or better yet, the network news protocol that enables USENET to function might include a norm that the system would not be used to distribute commercial advertisements.

Finally, we could imagine a pricing system for controlling how a network is used. The code could charge users based on the bandwidth used or on the amount of time connected. This was the technique, for example, of AOL for many years. It is the technique of many on-line service providers today.
These different techniques—whether architecture, or rules, or norms, or the market—all affect control over what gets used on a network. Control through architecture is just one kind. And since these techniques could overlap, a network could technically be end-to-end, at least from the perspective of the network architect, but because of other rules imposed through these different techniques, it would deviate from the values protected by end-to-end. If rules, norms, or the market vested control in the center, then the values of a decentralized, end-to-end architecture could be lost.

In this sense, the rules governing a network, whether through laws, contract, or norms, can function as a kind of intelligence in the network. This intelligence can be advantageous or not, just as architectural intelligence can be advantageous or not. But whether or not beneficial, my point so far to see is the change they effect over a network where resources are free.

**FAT PIPE**

Internet access across telephone lines is slow, even though modern technology has improved dramatically. When I first connected with a modem, I was happy to get a speed of 300 baud. My laptop modem now sends and receives data at up to 56,000 bits per second. But still, that speed is far too slow for the kinds of work people do on the network today. One can't surf the Internet quickly at even 56K, nor can one share large files quickly.

This limitation has pushed the market to supply faster and faster ways of getting access to the Net. And the most important new technology for getting fast access to the Net—at least in the immediate term—is "broadband" through cable lines.8

Cable technology was developed in the 1960s as a way of giving remote communities access to television.8 CATV stood for "community access television," and the very first installations simply placed an antenna on a mountain and ran a cable line down to a community in a valley. When it was first built, cable television was essentially an end-to-end system—there was little intelligence in the network; all the power was provided by the broadcaster and the TV; and both could be conceived to be at the ends. It was also essentially one-way, analog content. Television broadcasts were piped to TVs. There was no way for TVs to talk back.

Congress liked cable TV. The idea of spreading television to many was attractive to many politicians. So in the early 1970s, Congress and the FCC
began providing incentives for cable networks to be built. And among these incentives was a particularly lucrative asset—monopoly control.

The argument of the cable industry in favor of monopoly was simple: We need, they argued, incentives to risk the investment to build out cable TV. That build-out would be worth it to us only if we could be certain to recover our investment. This certainty would be adequately provided if we had complete control over the programming on our network. If we get to pick and choose the shows we run, and we get protected monopoly status in the local markets we run cable for, then we will have sufficient incentive to build out cable to secure our needs.

Not a bad deal, if you can get it. And even though "every major policy study on how cable should be regulated recommended that cable operators be required to provide at least some degree of non-discriminatory access to unaffiliated program suppliers,"9 Congress and the FCC ignored these recommendations. Cable was given control both over the physical infrastructure that built their network and over the code layer that made their network run.

From our perspective, however, there should be something odd about this decision. Telephones and television were both technologies that depended upon wires. Yet just as the nation was resolving to limit the control that the network owner had over one set of wires—telephone—it was increasing the control the network owner would have over a different set of wires—cable. From our perspective, these different policies for the same thing—wires—deserve an explanation, at least.

But at the time, telephones were as different from television as cars are different from buggies. It was not obvious to legislators (or if it was, they didn't let on) why the rules governing one should also govern the other. And even if it was obvious to some, the commercial pressure for exceptionalism was too great to resist. Just at the time America was coming to second-guess its first great network monopoly (telephones), it embraced and supported the construction of a second with the potential to be just as powerful.

So cable entered its golden years, which were brightened in the late 1970s only by the innovations of Ted Turner. Turner looked at cable and saw a waste of wires. Cable, he felt, could become a competing broadcasting network, not simply the supplicant to television broadcasters. So Turner bought access to a satellite and started broadcasting content across the satellite to cable stations everywhere. Cable thus became a content provider as well as a conduit for other people's content.10

By the early 1990s, cable was the dominant mode of accessing television
in America. It had gone from the farms to the centers of the largest cities. The number of stations increased dramatically, as the technology enabled hundreds of channels. And the range of channels exploded with the decrease in the number of viewers needed to make any particular channel succeed. When channels multiplied, the opportunity cost for each new channel fell; when opportunity costs fell, then uses of the networks increased.

Cable was about to hit a number of bumps in the road, however. Some were of its own creation—perceived “price gouging” led Congress twice to regulate the prices of cable services. But some it did not control. Satellite TV was the first of these; the Internet was the second.

Satellite TV offered competition to cable in the same way that cable had offered competition to TV. Services like DirecTV provided access to many more channels of television than cable, as well as the possibility to sell TV on a pay-per-view basis. Yet because it used no wires, the costs of providing this service were relatively low—at least when compared to cable. Thus, satellite provided a great challenge to the monopoly that cable was.

To respond to this competitive threat, cable needed to upgrade its systems to make it easier to supply two-way communication. Two-way communication was needed so consumers could make pay-per-view selections for television; fatter pipe would make it possible for cable to provide a wider range of content.

But while upgrading to compete with satellite, cable soon realized that it could also upgrade to provide two-way Internet service. And if it upgraded to provide Internet service, then cable could also be used to provide telephony. Thus the upgrade could secure cable in its primary market, while solidifying cable in these two new and growing markets.

**AT&T Cable**

To upgrade, however, would require a great deal of investment and, more significantly, technological development. First, there was no standard for enabling Internet across cable. Second, there was a great deal of poor-quality cable that needed to be upgraded. Some was quite old. And even the cable that was not old would require new technologies to make two-way cable work. So the cable companies formed an independent company—Cable Labs—to develop an open standard for serving cable. This standard—called the DOCSIS standard—would then be usable by modem providers that wanted to build cable modems to serve the growing Internet commu-
nity.13 And those with low-quality cable lines began replacing their lines with newer technology.

At first, and quite slowly, a number of local cable companies began to experiment with Internet access. An Internet access service provider, @Home, and Road Runner helped the cable systems come on-line. But soon the push for this change in technology came from an entity quite familiar with national communications networks: AT&T.

AT&T was looking for a way to get into the Internet market. In 1995, the Internet had just taken off; AT&T’s president, C. Michael Armstrong, decided AT&T had to be a part of the future. So AT&T devised a plan whereby it would purchase an interest in as many cable ventures as possible and slowly combine these cable systems under a single network enabled for broadband content. These networks, in turn, would be supported by selected ISPs—either @Home or Road Runner. Thus the design AT&T envisioned was of an Internet service network that would be supported by a limited number of Internet service providers—namely, those that it would control.

AT&T’s reasons for restricting its network to just two ISPs were many, and over time the reasons changed. The essence of its argument was that exclusive dealing with a small number of ISPs was “necessary.” At one point, they said it was “technically necessary”—claiming that it would be technically infeasible for AT&T to connect other Internet service providers to the AT&T network. But later, when other cable systems demonstrated how it might be done, AT&T claimed it was “economically necessary”—to give it adequate incentive to develop broadband cable.14

AT&T had eaten a bunch of cable monopolies and was now beginning to prove that you are what you eat: like the cable monopolies in the 1970s (and like AT&T in the 1920s), AT&T claimed a protected network was needed if broadband was to develop.

Cable was not, and is not, the only broadband game in town. Wireless, as I suggested in chapter 5, in principle could become an important competitor. And in many communities, cable has a competitor serving broadband across the telephone lines—DSL.

DSL (digital subscriber line) was developed many years ago.15 It is a way of transmitting data over a telephone line that is also being used for voice. The data is modulated above the frequency where voice service flows, so it doesn’t interfere with the telephone conversation. And in tests inside DSL
laboratories, there is some hope that it could transmit data at an extraordinarily high rate—52 megabits per second, by some estimates.\textsuperscript{16}

But DSL faces many hurdles, much like the hurdles that handicap cable. For a DSL connection to work, the copper wires in the local loop must be reasonably clean. This requires extensive work by telephone companies to find usable wires at the local loop. And it requires installing new routers no more than two miles from DSL customers. The cost of this upgrade to the copper wire world is huge, though some estimates that I have seen demonstrate that the per customer cost is the same for cable and DSL.

DSL does not have the option, however, of running a closed network. DSL is deployed by telephone companies. Telephone companies (by which I mean local Bells) are regulated to be open.\textsuperscript{17} That means that telephone companies must give ISPs the right to run their own DSL networks across the telephone companies' wires. And that means that the telephone companies' networks cannot exercise any real power over the kind of Internet service made available across their wires.

It might strike you as odd that the law would require one kind of broadband service—DSL—to remain open to other competitors, while allowing another broadband service—cable—to build the Internet of the future the way cable and telephones were built in the past. Why would the government permit control over the Internet in one case but require open competition in the other?

The answer is that there is no good reason for this inconsistency. It is solely a product of regulatory accident. The regulations governing telephones and all "telecommunications services" are found under Title II of the Communications Act of 1934. The regulations governing cable and all "cable services" are found under Title VI of the Communications Act. Title II requires open access to telecommunications services; Title VI does not. The telephone company is stuck with the position that DSL is a kind of telecommunications service. The cable companies have vigorously argued that broadband cable is not. And so far, though the battles are many, the law is in favor of cable. Cable companies have been allowed to limit the range of ISPs that use their wires, while the telephone company has been required to permit any number of ISPs to have access to its wires.

\textbf{But forget} what the law is for a moment. Which should it be? Should the lines be kept open, or should cable companies, and phone companies, be allowed to close the lines? Should the government do nothing to protect
openness in either case? Or should it consistently demand openness where closed systems reign?

Well, let's first be clear about what's at stake. Recall what end-to-end ensured: that the network would remain simple, and that it would be unable to discriminate against content or applications it didn't like, so that innovations—including those the network didn't like—would be possible on this network. That value is threatened if end-to-end on the Internet is compromised—either technically, by building control into the network (in ways that will become clear later on), or effectively, by layering onto the network rules or requirements that replicate this control. Whatever other closed and proprietary networks there might be, polluting the Internet with these systems of control is a certain way to undermine the innovation it inspires.

This is precisely what is happening on the cable networks right now. While the networks are being architected to be technically consistent with the principle of end-to-end, by requiring that everyone who gets access to cable do so through a small number of controlled ISPs, the cable companies will reserve to themselves the power to control what access they get—in particular, the power to decide whether some content will be favored over other content, whether some sites surf faster, and whether certain kinds of applications are permitted.16

And on the assumption that this control will be allowed, technology firms such as Cisco are developing technologies to enable this control. Rather than a neutral, nondiscriminatory Internet, they are deploying technologies to enable the "walled garden" Internet. The network is built to prefer content and applications within the garden; access to content and applications outside the garden is "disfavored." "Policy-based routing" replaces the neutral "best efforts" rule. The content favored by the policy becomes the content that flows most easily.17

Already cable has exercised this power to decide which kinds of applications should be permitted and which kinds not. As Jerome Saltzer, one of the coauthors of the "end-to-end" argument, describes, cable networks have already begun to be gatekeepers on the Net. As he writes:

Here are five examples of gatekeeping that have been reported by Internet customers of cable companies . . .:

1. Video limits. Some access providers limit the number of minutes that a customer may use a "streaming video" connection. . . . The
technical excuse for this restriction is that the provider doesn’t have
enough capacity for all customers to use streaming video at the same
time. But cable companies have a conflict of interest—they are re-
stricting a service that will someday directly compete with cable TV.

2. Server restrictions. While advertising the benefits of being “always
on” the Internet, some providers impose an “acceptable use” con-
tract that forbids customers from operating an Internet service, such
as a Web site. The technical excuse is that Web sites tend to attract
lots of traffic, and the provider doesn’t have enough capacity. But
again the access provider has a conflict of interest, because it also of-
fers a Web site hosting service. . . . (Some providers have adopted a
more subtle approach: they refuse to assign a stable Internet address
to home computers, thereby making it hard for the customer to offer
an Internet service that others can reliably find. And some access
providers have placed an artificial bottleneck on outbound data rates
to discourage people from running Internet services.)

3. Fixed backbone choice. Access providers choose where they attach
to a long distance carrier for the Internet, known as a “backbone
provider.” The route to the backbone provider and the choice of the
backbone provider are important decisions, bundled with the access
service. . . .

4. Filtering. Data is carried on the Internet in batches called packets,
and every Internet packet contains an identifier that gives a rough in-
dication of what this packet is for: e-mail, a Web page, a name
lookup, a remote login, or file sharing. Several access providers have
begun to examine every packet that they carry, and discard those
with certain purposes, particularly those used for file sharing. The
technical excuse for this filtering is that many users don’t realize that
their computer allows sharing of files, and filtering prevents other
customers from misusing that feature. But some access providers
have imposed filtering on every customer, including those who want
to share files. . . . And again, there can be a conflict of interest—the
access provider has an incentive to find a technical or political ex-
cuse to filter out services that compete with the entertainment or
Internet services it also offers.

5. No home network. An increasing number of homes have two or
more computers interconnected by a home network, and as time
goes on we are likely to find that this home network connects television sets, household appliances, and many other things. Some access providers have suggested that they aren’t technically prepared to attach home networks, but the technology for doing it was developed in the 1970’s. In refusing to attach home networks, providers are actually protecting their ability to assign the network address of the customer. By refusing to carry traffic to Internet addresses they didn’t assign, the access provider can prevent the customer from contracting for simultaneous service with any other Internet access provider.

The most telling of these limits is video. Cable companies make a lot of money streaming video to television sets. The Internet, in the view of some, could become a competitor to cable, by streaming video to computers. Under @Home rules, users were not permitted to stream more than ten minutes of video to their computers. And though AT&T offers congestion as a reason for this limitation, at times it is a bit more forthcoming. As AT&T executive Daniel Somers is reported to have said, when asked whether AT&T would permit the streaming of video to computers, “[W]e didn’t spend $56 billion on a cable network to have the blood sucked out of our veins.”

Cable’s intent to exercise control is clear; it has already exercised control. And if the business model that Cisco sells is as attractive as Cisco sells it to be, then we should expect that cable will continue to exercise control in the future. It will architect and enforce a network where the kinds of uses and content that run on the network are as the network chooses—which is to say, it will build a network just the opposite of the network the Internet originally was.

The evidence of this intent to discriminate was strongest at AT&T’s @Home media. As François Bar reports, “[T]he @Home 1998 annual report is very clear” on the strategy of discrimination. It proposed to steer its customers, unknowingly, toward merchants that partnered with @Home. It would do this through code and marketing—through placement of ads, as well as through “how do I” wizards that would direct customers to selected sites. Their reports “explain how they will provide superior quality performance to partnering merchants.” In this respect, Bar argues, “@Home is acting very much like Microsoft, using its control of the operating system’s architecture to favor some applications over others.” This closed-access control would allow cable owners to pursue only the exploration and devel-
opment of new technologies that directly benefit them. "This is not to say that no innovation will take place," Bar argues, "simply that only the technology trajectories that line up with their interest will be pursued." *\(^26\)

One choice about these trajectories is particularly important to highlight. Recall from chapter 8 my description of the emerging technologies of peer-to-peer. These technologies presume "peers"—that is, machines that are roughly equal. And though connection speeds on narrowband connections were slow, they were equal upstream and downstream.

Not so with the emerging technologies of broadband. Most of these technologies are faster downstream than they are upstream. Most broadcast more quickly than they receive.

Given the way the Internet is used right now, this imbalance makes good sense. E-mail and Web clicks going up take far less bandwidth than streaming video going down. Hence this structure makes sense of the uses of today—it is optimized, that is, for the uses of today.

But as with any optimization, what's good for today is not necessarily good for tomorrow. More important, how we optimize the network today will affect what good is possible tomorrow. Thus, as we optimize the network for this broadcasting mode, it becomes harder for the peer-to-peer structures to evolve. A world where users are servers doesn't scale well when the connection to the Internet is biased in favor of servers at the center.

Ordinarily, we don't have to worry much about this sort of thing in advance. The original PC market didn't care much about design; Apple Computer then changed that preference. The early PCs didn't have much capacity for sound. Later innovation created an incentive for the early PCs to change. The reason in both cases is the power of the market: as long as the market is free and competitive, these new uses will evolve as consumers want them.

In the context of broadband, however, there may well be a reason to be more skeptical about the market. If the concentrations in ownership continue as they have in the past few years (recently encouraged by an FCC that wants to take a more hands-off approach), then at a certain point there may be a strategic reason for these networks to resist the peer-to-peer way. By architecting networks to enable peer-to-peer, broadband providers will be reducing the power they have to direct users as they wish.

Here's an analogy that might suggest the point: Imagine you're a cable company serving twenty channels in your market. A new technology comes
along that would open up two hundred more channels on your cable system. This technology is, let's assume, relatively cheap, and with it you could be certain to increase your communications capability ten times over. But the catch is that the content on these two hundred channels will be provided by your customers. Would you, as the cable company, adopt this technology?

The answer is that it depends. If the cable company could charge its customers differently because they used these different channels—if they could make up for the loss they suffered because fewer were watching the twenty channels by charging something for the use of the two hundred channels—then the cable company in principle should have no problem with the new technology. Prices would be adjusted to assure that the revenues the cable company received were as high as they were before.

But there are three problems with this happy assumption as applied to the Net. First, customers don't notice that they are living within a closed system. If a travel site comes up slowly because it is not a favored site, the user is likely to consider this congestion, not something owing to the network. Second, the business model of some networks is based on "owning" the customer, not on charges for access. The last thing these business models can accept is an architecture that opens more channels. But third, and more important, even if there's a price at which the cable company would be willing to allow this new innovation, that price may be too high to inspire investment in this new form of innovation. The innovation that gets devoted to a free, neutral platform is different from the innovation that gets devoted to a platform where the platform owner can, down the road, simply change its mind.

We've seen this lesson before, and we're at a point where we can state a general claim: Where a disruptive technology emerges, there may be good reason not to extend the power of existing interests into power over that technology. That doesn't mean the new technology should be allowed to defeat the old or, at least, defeat the old for free. For example, no doubt the customers who use the "two hundred new channels" technology on the cable system should have to pay something for this new capacity. But the price they pay should not necessarily be within the control of the dinosaurs. Instead, while compensation is justified, control is not required. Or, better, separating control from compensation may well be a way to induce more innovation.
MY CLAIM so far can be summarized like this: When the Internet was first born, both norms (among core network facilities) and law (restricting the telephone company) effected an end-to-end environment. This created the initial neutral platform. But as the Internet moves to broadband platforms, neither norms nor the law require network providers to preserve the same innovation environment. The trend instead is toward control—toward layering onto the original code layer of the Internet new technologies that facilitate greater discrimination, and hence control, over the content and applications that can run on the Internet. The Net is thereby moving from the principle of end-to-end that defined its birth to something very different.27

MANY RESIST the view that this control is anything to worry about. Cable is just one of a number of broadband technologies. DSL, as I have noted, is not free to be closed. In many contexts, DSL competes with cable. Hence if consumers value openness, then they can choose DSL over cable. And if they choose DSL because DSL is open, then cable will be pressed to be open as well.28 Thus competitive forces will force the network to open up, even if cable desires to be closed.

I agree with this claim, as far as it goes. To the extent consumers prefer open to closed, they will put pressure on the closed providers to be open. But to move from that claim to the conclusion that therefore there is nothing to worry about is, in my view, premature. There are plenty of reasons to worry that the closed character of cable won’t correct itself.

First, there is the issue of numbers, and numbers of two sorts—the number of people on cable broadband, and the number and character of other broadband providers. Cable now has a great lead over DSL in subscribers to the cable system. There were 5 million cable broadband customers and 1.8 million DSL customers in 2000.29 Some predictions suggest that DSL may close in on cable by 2002,30 especially in nonresidential areas where cable does not now exist. But there are just as many who predict that cable will continue to lead.

But second, there is the number of different broadband providers and the character of their business models. For cable is not the only closed system. Wireless—the great hope from chapter 5—is being deployed now in a way that is primarily closed. The architecture for wireless broadband uses the same specifications that cable does—DOCSIS.31 DOCSIS, as you’ll re-
member, doesn't yet provide for simple open access. Thus the future is not
cable vs. DSL, but DSL vs. a scad of providers, all of which are closed.

Third, while DSL will be a strong competitor to simple Internet access,
cable access provides the opportunity to mix television content with Internet
content. And while DSL presses its limits to serve Internet as fast as
cable does, cable has a great deal of bandwidth that it can use to supply
Internet-related content. Right now cable provides 10 percent of its band-
width to be used for Internet service. It could easily multiply the number of
channels supplying Internet service and become a much more attractive op-
tion. Thus, while openness might be on DSL's side, the value of openness
to the consumer may be outweighed by the ability to bundle cable more ef-
fectively with other video content.

But fourth, and most important, consumers' preferences might not be
enough to motivate the market. This is the point we have seen both in chap-
ter 3's discussion of the value of e2e and in chapter 4's discussion of neutral
platforms: A closed network creates an externality on innovation generally.
It increases the cost of innovation by increasing the range of actors that
must license any new innovation. That cost is not borne directly by the con-
sumer. In the long run, of course, if it is a cost, it is borne by the consumer.
But in the short run, the consumer doesn't notice the innovation that the
closed model chills. Thus the consumer does not completely internalize
the costs imposed by a closed system. And hence the pressure the consumer
puts on closed systems to open themselves up is not equal to the costs that
such closed systems impose on innovation generally.

These are good reasons, I believe, for being skeptical about whether the
invisible hand will solve the problem of closed networks. The observation
that never in the history of telecommunications has a network voluntarily
been opened after being closed is another reason to be skeptical. Finally,
the interest of those who own these networks to keep control within the net-
work is huge, and a huge reason to be skeptical about their control.

To see this part of the story, however, we need to shift to a different battle
about open architectures—AOL.

America Online was born far from the Internet. Its birth was as an on-
line service that gave members access to other members. While other ser-
vice were focused on how to sell product, AOL understood from the very
beginning that networks are built by communities.

AOL's community was built by making computers easy and access simple.
The company “carpet-bombed” America with AOL disks; it made sign-up simple and access cheap. Quickly AOL built a following that was extraordinary for on-line services.\textsuperscript{32}

The AOL network was not really end-to-end. Lots of intelligence was built into the software with which one connected to AOL. AOL made that intelligence work to assure ease of access as well as control where control was needed. The service held the user’s hand, but it required some intelligence to know where the hands were. It was a preprogrammed world, which users took as they found it. No one built additions to AOL or added functionality to AOL without AOL’s permission.

That wasn’t the case with all on-line communities. MUDs (multi-user domains), for example, were on-line communities where people were free to develop new parts of the on-line, virtual, text-based world.\textsuperscript{33} If you wanted to add a room to an existing MUD, you simply wrote the code to add the room and submitted it. The space that got built was as the members built it.

In AOL, the only building was that approved by the town planner—AOL. And AOL succeeded in building an extraordinarily popular place.

When the Internet came along, many thought AOL would die. Why pay to get access to preselected content when you could get access much more cheaply to the Internet as a whole? But AOL responded to this challenge by doing what it does best: by building its service to make it easy for users to find their way onto the Internet. The Internet was one place AOL users could go, but then there was also the content on AOL. Both would be available to AOL customers; only the Internet was available to others.

AOL then became another Internet service provider, but with something extra that came from the content it served. It was an ISP plus, because it also had its own content. But many simply used the service to get easy access to the Internet. And AOL then was subject to the fierce competition that every ISP faced. With some five thousand ISPs across America, there was only so much power any one ISP had—even if that ISP had a very large number of customers.

AOL was built on narrowband telephone lines. When broadband came along, AOL faced a critical threat. If broadband service was reserved to just two ISPs, and if it was far superior to the service one could get across the telephone lines, then AOL faced a great challenge from this emerging Internet opportunity. If AOL was barred from broadband, then AOL would be history.
AOL thus joined many who were pushing the FCC as well as local governments to require that broadband cable lines be kept open for competition. This was the “open access” movement; AOL was a key player. In 1999, AOL argued to the city of San Francisco during its open access implementation hearings:

AOL applauds the City for taking this critical step in the implementation of the Board of Supervisors’ open access resolution, which wisely supports consumers’ freedom to choose their Internet service provider and to access any content they desire — unimpeded by the cable operator.  

AOL had made the same arguments in favor of governmental intervention to the FCC. In this campaign, AOL’s allies were many. Indeed, before AT&T started buying cable lines, AT&T too was an ally. In Canada, AT&T argued to the Canadian government that access to cable in Canada should be regulated to be open.

AT&T Canada LDS submits that the application of the Commission’s forbearance test to the two separate markets for broadband access and information services supports a finding that there is insufficient competition in the market for broadband access services and the market for information services to warrant forbearance at this time from the regulation of services when they are provided by broadcast carriers. As noted above, these carriers have the ability to exercise market power by controlling access to bottleneck facilities required by other service providers. It would appear, therefore, that if these services were deregulated at this time, it would likely impair the development of competition in this market as well as in upstream markets for which such services are essential inputs.

Vertically integrated cable and telephone facility owners, AT&T had argued, possessed market power and had to be prevented from engaging in anticompetitive practices.

But when AT&T bought its own cable lines, its story changed. No longer did it believe that cable should be regulated. Instead, AT&T began to argue that the market should regulate cable, and the government should stand aside.

This would become a familiar pattern.

In January 2000, AOL and Time Warner announced to a startled world that they had agreed to merge. Time Warner owned many cable companies;
these cable companies would serve AOL content at high speed. AOL had many Internet customers. These customers would be able to get access to Time Warner content. The merger was an ideal opportunity, both companies argued, for synergy in this market. The old and the new would form together one of the most important media companies in the world.

At the same time, AOL announced its policy on open access had changed. It, like AT&T, no longer believed that the government should regulate access. It, like AT&T, believed that the market should regulate itself.38

I’m not sure why people are surprised by flips in corporate policy, any more than we are surprised by flips of politicians. Corporations have a duty to their shareholders. Their job is to make money. If the opportunities present themselves, they will, and should, change their views. They are not institutions of public policy. And they don’t deserve the attack that would befall an institution of public policy that so radically, and transparently, switched sides.

But the other side of this obvious point is that we should not treat what corporations say is good public policy as what is good public policy. We should treat them as statements by individuals who are required by law to be self-serving. This is not just “bias”—this is legally mandated bias.

Thus, I discount both AOL’s support and AOL’s opposition to government regulations to support open access as evidence about whether open access is good policy. The question is not what AOL believes is good for AOL. The question is what is good for the Internet.

And here again we return to the question, What trend should we expect? The opponents of any governmental role here argue that the market will take care of itself. I think that’s true—the market will take care of itself. AOL/TW will build itself to maximize its market power. The question is what shape that building will take.

The danger is what economists would call the problems of vertical integration—where one provider controls the full range of services across the layers I described—content, logical, and physical.39 Outside the Internet, the danger of vertical integration is less.40 But within a network, the danger grows. Such integration, a report by the National Research Council has concluded, “could, if successful, cause a change in the Internet market,
with innovation and creativity becoming more the province of vertically integrated corporations. It would, Web founder Tim Berners-Lee worries, be dangerous for innovation generally. “Keeping the medium and the content separate,” Berners-Lee writes, “is a good rule in most media. When I turn on the television, I don’t expect it to deliberately jump to a particular channel, or to give a better picture when I choose a channel that has the ‘right’ commercials. I expect my television to be an impartial box. I also expect the same neutrality of software.”

The danger with the AOL-Time Warner merger is the danger that this vertical integration will induce AOL/TW to engage in discrimination—both discrimination in conduits (favoring their own lines over others) and discrimination in content (favoring their own content over others).

This danger is real. As economists Daniel Rubinfeld and Hal Singer have concluded, given the existing concentration in cable broadband, AOL/TW will have a significant incentive to engage in both forms of discrimination. And by mid-2001, AOL Time Warner had begun to prohibit advertisements on their sites for competing Internet access providers. Discrimination was threatened; discrimination is being realized.

As the Clinton administration came to an end, one of the last acts of the (by statute, at least, neutral) Federal Trade Commission (FTC) was a sign of some hope. After a long and extensive investigation into the risks of the proposed AOL-Time Warner merger, the FTC, led by its chairman, Robert Pitofsky, conditioned the merger of AOL and Time Warner upon the essential elements of open access. Access to the cable broadband pipes must be kept open, the FTC insisted. Nonaffiliated content must flow without hindrance from AOL or Time Warner. And this unhindered access must include access to Internet-active TV.

This decision by the FTC was an important breakthrough in the attitude of the government. Until this point, the government’s view had been that the market here had to take care of itself. The problem, as the increasing mergers and restrictive access conditions demonstrated, was that the market was taking care of itself. The market was building a protection into the architecture that could change the commons for innovation dramatically.

But this decision is just a first round. (And as I describe in Chapter 11, this first round may well be overturned by the courts.) As cable gets built out, as an administration emerges that is more open to allowing the market rather than rules to regulate, as other modes of broadband are built, the constant
pressure will be to allow this founding principle of neutrality to itself be neutralized.

And then the question becomes this: If the original Internet architected an innovation space that was free, if it built that space by creating an environment where innovations would not be checked, if it was defined by a code layer that, in Benkler’s terms, was open, then as the Internet moves onto fat pipes, will the same principle govern the code layer of the Net? Will broadband respect the principle of end-to-end as narrowband has? And if it doesn’t, will the government do anything to resist the change?

What’s at stake here are two models for organizing a communications network, and the choice for us is which model will prevail. On the one hand, there is the model of the perfectly controlled cable provider—owning and controlling the physical, logical, and content layers of its network. On the other hand, there is the model of the Internet—which exerts no control over a physical layer beyond the decision to include equipment or not, and which enables the free exchange of content over a code layer that remains open.

As the Internet moves from the telephone wires to cable, which model should govern? When you buy a book from Amazon.com, you don’t expect AOL to demand a cut. When you run a search at Yahoo!, you don’t expect your MSN network to slow down anti-Microsoft sites. You don’t expect that because the norm of neutrality on the Internet is so strong. Providers provide access to a network that is neutral. That’s the essence of what the Internet means.

But the same neutrality does not guide our thinking about cable. If the cable companies prefer some content over others, that’s the natural image of a cable provider. If your provider declines to show certain stations, that’s the sort of freedom we imagine it should have. Discrimination and choice are at the core of what a cable monopoly does; neutrality here seems silly.

So which model should govern when the Internet moves to cable? Freedom or control?

Not every increase in control violates the principle of end-to-end. Obviously the ends are free, as far as this principle is concerned, to do what they want with their machines, and while some would resist calling the cable networks an “end,” they could well argue that they are just a private network
connected to the Internet. To link to the network is not to commit your hard
disk to the use of anyone. The physical layer remains controlled, even if the
code layer is free.

Here we see the source of the compromise that this chapter is all about.
For in an important sense, the cable network is simply asserting the same
rights with “its” equipment that I assert over my machine when connected
to the Internet. My machine is mine; I’m not required to make it open to
the world. To the extent I leave it open, good for the world. But nothing
compels me to support it.

Leaving the ends free to choose, then, creates an opportunity for them to
choose control where the norm of the Internet has been freedom. And con-
trol will be exercised when control is in the interest of the ends. When it
benefits the ends to restrict access, when it benefits the ends to discriminate,
then the ends will restrict and discriminate regardless of the effect on others.

Here, then, we have the beginnings of a classic “tragedy of the com-
mons.”46 For if keeping the network as a commons provides a benefit to all,
yet closing individual links in the network provides a benefit to individuals,
then by the logic that Garrett Hardin describes in chapter 2 above, we
should expect the network “naturally” to slide from dot.commons to
dot.control. We should expect these private incentives for control to dis-
place the public benefit of neutrality.47

The closing of the network by the cable companies at the code layer is
one example of this slide. If DSL providers were given the choice, they too
would do the same. Wireless providers are implementing essentially the
same sort of control. AOL Time Warner is insisting that code using its net-
work be code that it controls.

In all these cases, the pressure to exert control is strong; each step makes
sense for each company. The effect on innovation is nowhere reckoned.
The value of the innovation commons that dot.commons produces is whitt-
tled away as the dot.coms rebuild the assumptions of the original Net.

Consider another example of this tragedy in play:

The World Wide Web is crawling with spiders. These spiders capture
content and carry it back to a home site. The most common kind of spider
is one that indexes the contents of a site. The spider will come to a Web
page, index the words on that Web page, and then follow the links on the
Web page to other sites. And by following this process as far as the links go,
these spiders index the Web.

This index, then, is what you use when you run a search on the Web.
There are many Web search engines, each with a slightly different technique. But they all rely upon the ability to spider the Web and gather the data the Web makes available.

These "spiders" are also called "bots." A bot is simply a computer program that runs remotely on another machine. Searching is just one example of the kinds of things computer "bots" do to one another on the Web. Some of those other things are awful: "denial of service attack" is an event where either one or a number of coordinating computers sends repeated requests to a Web page, ultimately overwhelming the server for that page. But in the main, these "things computers do to each other" have been productive and extraordinarily creative.

One example of this creativity comes in the context of auction sites. Auction sites make products available to real-time, wide-scale auctions. eBay is the most famous, but not the only one. eBay opened in 1995 as a place where individuals could offer their stuff in an auction to others. The idea caught on, and competing sites started offering the same service. Amazon.com has its own auction site, as does Yahoo!.

But then customers interested in auctions faced another "metaproblem." If they had things they were watching on many different sites, they had the hassle of traipsing through all those sites to find what they wanted to watch. So where there was a problem, the market quickly provided a response. Bidder's Edge, among others, began to offer a site that did the surfing for you. On one page you could see the status of all your auctions. And Bidder's Edge promised to update this information regularly.

In each case, the innovation is the same. The Web is an open architecture; it begs for people to discover new ways to combine the resources it makes available. In each of these cases, someone did discover a new way of combining resources. And this discovery then produced a new kind of market. Search engines were a defining feature of the original World Wide Web. And the opportunity to quickly compare prices was one of the early promises for competition on the Web.

But in each case, too, there is this undeniable fact: When a search engine spiders the Web, it uses resources of others to build its index. When Best Book Buys enters Amazon.com, it collects the price Amazon offers by using Amazon's servers. In a sense, then, we could say that each of these bots trespasses on the servers of other sites.

To many, this idea of trespassing bots will seem bizarre. But it did not seem too bizarre to the lawyers at eBay. For eBay didn't want bots that cre-
ated competitors to eBay. And it had imposed a NO-BOT policy on access to its Web site. That is, it indicated in the code of its site that it did not want unlicensed bots to enter its site.

Bidder's Edge ignored that sign. It continued to gather data even though the eBay lawyers told it not to. And eventually it found itself in court, in a lawsuit brought by eBay charging Bidder's Edge with "trespas."

In one sense, of course, the lawsuit was completely right. In the virtual sense in which one "goes" to a Web site, Bidder's Edge's bot was "entering" a computer without the permission of its owner. And "entering" without permission is the classic definition of "trespass."

But in another sense, the claim seemed bizarre. The Web was built on a norm of open access; this was a community that kept its doors unlocked. No one forced eBay to open itself to the World Wide Web. But if it did, it should live by the norm. And if the norm was openness, then it was eBay that committed the offense.

Both sides brought in lawyers to argue their respective points of view. On the side of eBay was an outspoken, and famous, law professor from the University of Chicago—Richard Epstein. Epstein pushed the law-focused answer: Trespass law made perfect sense in the Internet context. Indeed, it made more sense here than in real space. It was simple to establish signs that stated the conditions under which entry was permitted; those signs could be easily read by bots. If a site wanted to restrict access to all save those who pay, then that was perfectly permissible, Epstein argued. The site, after all, "owned" the equipment. Control over the property one owns is perfectly ordinary.46

On the other side was a lawyer who was a bit more careful with the legal tradition. Law professor Dan Burk argued that the law had been strict only when it came to "land." Other property was protected against unauthorized use. But that protection was not absolute. To support a lawsuit based on trespass to property other than land, the plaintiff would have to demonstrate some sort of harm. But in the Bidder's Edge case, no harm had been pleaded. Thus, under traditional trespass doctrine, eBay should lose.

Both sides had a point, and while my bias is with Burk, I don't mean to deny the plausibility of a different regime. What I do deny, however, is that the answer to this question is obvious. What is most damaging about the submission made by Epstein is its obliviousness to any issue on the other side.

For no doubt we could move to a world where every use of data on the Web had to be licensed. We could generalize from the control everyone has
over "his" machine to the power to deny the neutrality of the network generally.

But there are costs to that world. Closing access based on this argument grounded in the physical layer of the Net increases the costs of innovation for the Net generally. If to deploy a technology the innovator must first license its use, this legal requirement then functions as a kind of tax on innovation on the Net.

This is especially true with bot technologies. These devices—the next generation after the spiders that gather data from the Net—would enable agent-driven, fluid marketplaces on the Net. These bots could search out prices, negotiate contracts, and schedule delivery in a way that is far more efficient than any of the existing markets.49

The response to this is that we don't want rules that force people to devote their resources to something they don't want to support. Bidder's Edge didn't pay the servers that it used when it linked to eBay's data. Why should eBay be forced to subsidize a competitor?

But this story could be told both ways around. eBay benefits greatly from a network that is open and where access is free. It is this general feature of the Net that makes the Net so valuable to users and a source of great innovation. And to the extent that individual sites begin to impose their own rules of exclusion, the value of the network as a network declines. If machines must negotiate before entering any individual site, then the costs of using the network climb.

As I said at the start, this closing of sites selectively changes the character of the Net, but not necessarily its compliance with end-to-end. As it increases, however, it does change the commons of the Internet into something different. To the extent that this ability—to select the uses that access to the Net permits—grows, then this permission changes the character of the commons the Internet creates.

This discrimination is growing in other contexts as well. Sometimes it happens for innocent reasons, sometimes less innocently. An innocent case is the emergence of a technology called "network address technologies" (NATs). NATs are devices for multiplying IP addresses. Every machine on the Internet needs a unique IP address—that's how the Net knows where to send the packets. But NATs make it so many machines can share the same IP address.

NATs were created initially because of an expected shortage of IP ad-
addresses. The technology has subsequently grown simply because of the difficulty in coordinating devices in many contexts. Apple, for example, uses NATs to connect machines to its AirPort wireless server. You can plug an AirPort into your cable or DSL modem and then an unspecified number of machines can share the very same IP address.

The problem with NATs is that the techniques used to share IP addresses are not standard. The NAT inserts points of control into the network. Data passing onto a NAT-controlled network must pass through the NAT before the NAT permits it to pass to the end user. If the NAT is unaware of how to process the data from that particular application (either because the NAT was unaware of that application or because it was coded to ignore data of that type), then that application won’t function on that NAT-empowered network. Developers of technologies that need to be certain they are talking to a particular machine must therefore survey the world of NATs to make certain their systems will work on all the major brands. This in turn increases the costs of development and, on the margin, may reduce innovation.

No one thinks NAT boxes are part of a conspiracy. This compromise of end-to-end is innocent in the sense that we don’t imagine it is implemented for strategic purposes. Nonetheless, it reduces the flexibility of the Internet as a whole.

But there is a solution to the problem that NATs were initially designed to solve—and again, it is to increase capacity. The name space for the Internet (IPv4) is in the process of being upgraded (to IPv6). That will have a practically endless number of addresses, thereby eliminating the need for NATs. With endless address space, technologies for “conserving” addresses become unnecessary at best. Thus, rather than imposing this high-coordination cost on technologists developing technology for the Net, increasing the name space would remove the initial reason for the compromise.

Other compromises with end-to-end are less benign. Consider firewalls, for example. A firewall is a technology for controlling interaction between a local network and the Internet. Like the NAT, it is a technology that adds a point of control within the network that could block everything that has not explicitly been admitted by the local network manager. Unforeseen applications thus again pay a heavy price.

Firewall technology, for example, no doubt serves a legitimate purpose in many cases. Sometimes, however, its purpose is expressly to impose a policy on the Net. Many universities, for example, forbid the use of Napster tech-
nologies. They enforce this ban by telling their firewalls to block Napster content. This in turn produces something of an arms race, as developers shift their systems to channels that will never be filtered by a firewall. But that shift will only make it harder to use those channels in different applications efficiently.\textsuperscript{51}

Here too there is a solution that could solve the problem that firewalls answer, but without compromising end-to-end. A technology called IPSec could enable better control over access consistent with end-to-end.\textsuperscript{52}

In each of these cases, then, there are two issues at stake. As technologies for facilitating discrimination increase, one question is where these technologies get located in the Net—on the Net or at the edge. A second question is the effect such discrimination will have, even if it is located at the ends. The end-to-end principle counsels that we locate such discrimination at the ends rather than in the network; but even when it is located at the ends, a widespread pattern of certain types of discrimination could weaken the commons the network now provides.

There are reasons not to worry so much about this kind of discrimination. Where concentration is slight and many different services are available, the risk that any particular concentration will harm innovation is slight as well. Some ends may be Christian Right; as long as they don’t interfere with access to the Christian Left, innovation for the Christian Left will not be harmed. The key is to preserve user autonomy; the danger is a technology that might undermine autonomy.

The danger is discrimination engaged in by concentrated actors. Here again we return to the story of concentrating cable. For if we were in a world where there was significant competition in broadband services, with many different suppliers each essentially open—and hence, each not discriminating in the kind of access that is provided—then the danger from closed access in one channel would be greatly reduced. The value of the commons in the highway is not lost simply because some roads become private. But when there isn’t a great deal of competition in access, when a small number of companies can set the rules for the whole system, then the dangers in discrimination return. When a few can make decisions about what kinds of innovation will be permitted, the innovation promised by an end-to-end architecture is lost.

The danger of the changes that I have described in this chapter is that just this concentration is occurring. And the dangers in this concentration include the fear that an opportunity for innovation will be lost. We will have used architecture and rules to shift control over how the network can be
used, from the many ends that constituted the Internet originally, to a few that own the wires. Control will have been returned to this medium born free.

There is another side to the stories I have told. Not every increase in control is driven by a desire to lessen competition; not every increase will have the effect of undermining innovation.

Indeed, some increase in control may well be necessary if investment to build a network is to proceed. Just as cable companies argued initially that control over their cable lines was essential if there were to be a sufficient return from laying cable, so too cable companies today may rightly argue that control is needed if the return is to be enough.

The cable companies may be right. And striking a monopoly deal with a provider is a strategy that governments have employed since the start of governments. My argument cannot begin to resolve the question of whether or not the cable companies are right in their defense. If this infrastructure is to be built without public support, then protected monopoly may well be necessary.

My argument is meant simply to highlight a cost that may well run with a benefit. The Internet is not a community antenna. It is not simply a system for delivering a given kind of content more efficiently. The critical feature of the Internet that sets it apart from every other network before it is that it could be a platform upon which a whole world of activity might be built. The Internet is not a fancy cable television system; the Internet is the highway system, or the system of public roads, carrying bits rather than trucks, but carrying them in ways no one can predict.

When the United States built its highway system, we might have imagined that rather than fund the highways through public resources, the government might have turned to Detroit and said, Build it as you wish, and we will protect your right to build it to benefit you. We might then imagine roads over which only American cars can run efficiently, or exits and entrances that tilt against anything built outside Detroit. Or we could imagine Detroit then auctioning rights to use its network to the highest bidder, or excluding Coke trucks because of an exclusive contract with Pepsi.

This power in Detroit might well have been necessary if Detroit were to have had sufficient incentive to build the highways. But it does not follow that Detroit should be given this power. For however much the state may
gain by not having to fund roads on its own, society would lose in the aggregate if the open commons of transportation were lost.

That loss is even more pronounced in the context of the Internet. Roads have many uses, but “many” is still not infinite. Any kind of commerce gets to use the roads: trucks as well as VW bugs; campers as well as pickups. But the physical nature of roads limits the possible “many” uses. Lots are possible, but “the possible” is constrained.

The constraints on the Internet—properly architected—are far fewer. The range of uses is far less constrained. The Internet could be a platform for innovation across the full range of social and political life. Its possible uses are, even this far into its growth, unknowable.

We may gain something by giving network owners power over the network. I don’t question that. But we will lose something as well. To the extent we chill innovation that threatens disruption, disruption will be slower in coming. That slowness is a cost that society must account for. We may gain something from the “free” infrastructure monopoly builds. But we lose something with the “controlled” infrastructure that monopoly inevitably wants.

Even more significant, we have no good way to make sure that the gains outweigh the losses. To the extent that the code layer builds an innovation commons, changes at the code layer threaten to exhaust that commons. Changes imposed by broadband providers weaken the value of the neutral platform; changes effected through NATs or firewalls similarly weaken the innovation potential of the Net. All these changes are effected locally, but they also have a global effect. Each may make sense locally, but there’s no obvious way to be certain that their effect globally will also make sense.

In this way, changes at the code layer create their own tragedy of the innovation commons. As we might paraphrase Hardin:

Therein is the tragedy. Each [firm] is locked into a system that compels [it] to increase [its control] without limit—in a world that is limited. Ruin is the destination toward which all [firms] rush, each pursuing [its] own best interest in a society that believes in the freedom of the commons. Freedom in a commons brings ruin to all.33

“Ruin” is a strong word, I’ll concede. But the dynamic is the same nonetheless: the incentive is for companies to layer control onto the Net; that has been the history of the past five years. But the effect of that incen-
tive is felt by the Net as a whole. Yet its effect on the innovation commons is almost completely ignored.

Against this trend, some rightly argue that government has a role to play to assure that ISPs continue to offer “open IP service.” As a recent National Research Council report put it:

[C]oncerns about the vertical integration of the data transport and content businesses and about content control, as seen in recent debates about access to cable broadband Internet systems, could be eased if ISPs committed to providing their customers with open IP service. From this standpoint, the continued delivery of open IP service would be an enlightened move in the long-term interest of the industry.54

Just the sort of wisdom that finds its way into NRC reports and is ignored almost everywhere else.

The change that is happening in the context of wires has a particular form. We are in the midst of a radical change in technology; that change threatens existing interests; those interests have an interest in minimizing the threat that this change presents; they can minimize that threat by reestablishing choke points on the system that emerges. They can, in the words of Gerald Faulhaber, use the architecture to regain strategic control.55

This is precisely the change that is happening. As Charles Platt put it in a recent article in Wired, “Everyone knows that the broadband era will breed a new generation of online services, but this is only half the story. Like any innovation, broadband will inflict major changes on its environment. It will destroy, once and for all, the egalitarian vision of the Internet.”56

Dinosaurs should die. This lesson we have learned over and over again. And innovators should resist efforts by dinosaurs to keep control. Not because dinosaurs are evil; not because they can’t change; but because the greatest innovation will come from those outside these old institutions. Whatever the scientists at Bell Labs understood, AT&T didn’t get it. Some may offer a theory to explain why AT&T wouldn’t get it. But this is a point most understand without needing to invoke a fancy theory.

Because the Internet is inherently mixed—because it is a commons built upon a layer that is controlled—this tension between the free and the controlled is perpetual. The need for balance is likewise perpetual. But the value of balance is not always seen. This value we need to keep in focus.
Controlling the Wired

(and Hence the Content Layer)

In the last chapter, I argued that there is a tension between control at the physical layer and freedom at the code layer, and that this tension affects the incentives for innovation. The original freedom built a commons; more control can undermine that commons; the tragedy is our forgetting the value of the free in our race to perfect control.

The same tension exists at the content layer. Some content the law treats as “owned” — copyright and patents are “intellectual property,” owned by individuals and corporations. Other content can’t be owned — either content that has fallen into the public domain or content that is outside the scope of Congress’s power under the copyright and patent clause of the Constitution. Here, too, balance is important. Yet here, too, the owned chases out the unowned. The pressure to protect the controlled is increasingly undermining the scope for the free.

My aim in this chapter is to describe this dynamic and to suggest how changes that we are seeing right now will affect this dynamic. By the time this book is published, I fear the struggle I am describing will be finished. The courts will have resolved these questions, and the politicians will have no courage to interfere with this resolve. Already the endgame is clear; already property has queered the balance. Hence, already the value of this freedom will have been lost.

This chapter is meant to mirror chapter 4, “Commons Among the Wired.” Yet it is not directly about the people I spoke of in chapter 4. The
“wired” who are affected by the changes I am describing here are not exactly the same “wired” who built the open source and free software movements that I spoke about there.

But in a critical sense, they are the same. Both innovate by building on the content that has gone before. Both therefore reveal how much creativity depends upon the creativity that has gone before. Both show, that is, innovation as adding something to the work of others.

In some cases, the restrictions I describe in this chapter apply directly to the innovators of chapter 4. Patent law, for example, poses one of the most significant threats to the open code movement that there is. But in general, the changes I describe in this chapter are aimed at controlling a new generation of “wired” folks—those who see the platform of the Internet as an opportunity for a different way of producing and distributing content and those who see the content on the Net as a resource for making better and different content. The changes in this chapter are changes that reestablish control over this class of potentially wired souls.

When the Net emerged into the popular press, there was an anxiety among many about what the Net would make possible. People could do things there that we had discouraged or made illegal here.

Pornography was the most dramatic example of this anxiety. The freedom of the Net meant, the world quickly learned, the freedom of anyone—regardless of age—to read the obscene. The news was filled with instances of kids getting access to material deemed “harmful to minors.” The demand of many was that Congress do something to respond.

In 1996, Congress did respond, by passing the Communications Decency Act (CDA). Its aim was to protect children from “indecent content” in cyberspace. The act was stupidly drafted, practically impaling itself upon the First Amendment, but its aim was nothing new. Laws have long been used to protect children from material deemed “harmful to minors.” Congress was attempting to extend that protection here.

Congress failed. It failed because the CDA was overbroad, regulating speech that could not be regulated constitutionally. And it failed because it had not properly considered the burden this regulation would impose upon activity in cyberspace. The statute required adult IDs before adult content could be made available. But to require sites to keep and run ID machines was to burden Internet speech too severely. Congress would have to guarantee that the burden it was imposing on the Internet generally was no
greater than necessary to advance its legitimate state interest—protecting children.

In 1998, Congress tried again. This time it focused on clearly regulable speech—speech that was "harmful to minors." And it was much more forgiving about the technology that would permissibly block kids from "harmful to minors" speech. Still, federal courts struck down the law on the ground that the burden it would impose on the Internet generally was just too great.  

These cases evince a distinctive attitude. Though the state's interest in protecting children is compelling, courts have insisted that this compelling state interest be pursued with care. In effect, a demonstration that the regulation won't harm the Net too broadly is required before this state interest can be promoted. Facts, and patient review, are the rule in this area of the law of cyberspace.

Keep this picture in mind as we work through the examples that follow. For the meaning of Reno v. ACLU is not that porn is okay for kids or that the state's interest in enabling parents to protect their kids from porn is outdated. The Court in Reno was quite explicit: Protecting children from speech harmful to minors is a "compelling" state interest. But this compelling interest must be advanced in ways that are consistent with the other free speech values. The state was free to advance its compelling state interest; but it was required, in so doing, not to kill the rest of the Net.

About the same time that parents were panicking about porn on the Net, copyright holders were panicking about copyright on the Net. Just as parents worried that there was no way to keep control over their kids, copyright holders worried that there was no way to keep control over copyrighted content. The same features of the Internet that made it hard to keep kids from porn also made it hard to keep copyrights under control.

Both forms of panicking were premature. While it is true that the Net as it was originally built made it hard to control content (by either keeping it from kids or keeping it from being copied by kids), the Net as it was originally built is not the Net as it must be. Code made the Net as it was; that code could change. And the real issue for policy makers should be whether we can expect code to be developed that would solve this problem of control.

In Code I argued that in the context of copyright, we should certainly expect such code to be developed. And if it were developed as its architects
described, then the real danger, I argued, is not that copyrighted material would be uncontrolled: the real danger is that copyrighted material would be too perfectly controlled. That the technologies that were possible and that were being deployed would give content owners more control over copyrighted material than the law of copyright ever intended.

This is precisely what we have seen in the past two years, but with a twist that I never expected. Content providers have been eager to deploy code to protect content; that much I and others expected. But now, not only Congress but also the courts have been doubly eager to back up their protections with law.

This part I didn’t predict. And indeed, in light of Reno v. ACLU, one would be justified in not predicting it. If parents must go slowly before demanding that the law protect their kids, why would we expect Hollywood to get expedited service?

The answer to that question is best left until after we have surveyed the field. So consider the work of the courts, legislatures, and code writers in their crusade to expand the protections for a kind of “property” called IP.

INCREASING CONTROL

Copyright Bots

IN DORM rooms around the country, there are taped copies of old LPs. Taped to the windows, there are posters of rock stars. Books borrowed from friends are on the shelves in some of these rooms. Photocopies of class material, or chapters from assigned texts, are strewn across the floor. In some of these rooms, fans live; they have lyrics to favorite songs scribbled on notepads; they may have pictures of favorite cartoon characters pinned to the wall. Their computer may have icons based on characters from The Simpsons.

The content in these dorm rooms is being used without direct compensation to the original creator. No doubt, no permission was granted for the taping of the LPs. Posters displayed to the public are not displayed with the permission of the poster producers. Books may have been purchased, but there was no contract forbidding passing them to other friends. Photocopying goes on without anyone knowing what gets copied. The lyrics from songs copied down from a recording are not copied with the permission of the original author. Cartoon characters, the exclusive right of their authors,
are not copied and posted, on walls or on computer desktops, with the permission of anyone.

All these uses occur without the express permission of the copyright holder. They are unlicensed and uncompensated ways in which copyrighted works get used.

Not all of these uses are impermissible uses. Many are protected by exceptions built into the Copyright Act. When you buy a book, you are free to loan it to someone else. You are free to copy a small section of the book and give it to a friend. Under the Audio Home Recording Act, you are free to copy music from one medium to another. Taped recordings of records are therefore quite legal.

But some of these uses of copyrighted works may well be illegal. To post the poster may be a public display of the poster not authorized by the purchase. To use icons on your computer of Simpsons cartoons is said by Fox to violate its rights. And if too much of an assigned text has simply been copied by the student, then that copying may well exceed the scope of “fair use.”

The reality of dorm rooms, however—and, for that matter, most private space in real space—is that these violations, if they are violations, don’t matter much. Whether or not the law technically gives a student the right to have a Simpsons cartoon on his desktop, there is no practical way for Fox Broadcasting Company to enforce its rights against overeager fans. The friction of real space sets the law of real space. And that friction means that for most of these “violations,” there is no meaningful violation at all.

Now imagine all this activity moved to cyberspace. Rather than a dorm room, imagine that a student builds a home page. Rather than taped LPs, imagine he produces MP3 translations of the original records. The Simpsons cartoon is no longer just on his desktop; imagine it is also on his Web server. And likewise with the poster: the rock star, we can imagine, is now scanned into an image file and introduces this student’s Web page.

How have things changed?

Well, in one sense, one might say the change is quite dramatic. Now, rather than simply posting this content to a few friends who might pass through the dorm room, this student is making this content available to millions around the world. After all, pages on the World Wide Web are available anywhere in the world. Millions use the World Wide Web. Millions can now, for free, download the content that this student posted.

But there’s a gap in this logic. There are millions who use the World
Wide Web. But there are billions of Web pages. The chances that anyone will stumble across this student's page are quite slight. Search engines balance this point, though that depends upon what's on a particular page. Most Web pages are not even seen by the author's mother. The World Wide Web has amazing potential for publishing; but a potential is not a million-hit site.

Thus, in reality, this page is effectively the same as the student's dorm room. Probably more people view the poster on the dorm room window than will wade through the student's Web page. In terms of exposure, then, moving to cyberspace doesn't change much.

But in terms of the capacity for monitoring the use of this copyrighted material, the change in the move from real space to cyberspace is quite significant. The dorm room in cyberspace is subject to a kind of monitoring that the dorm room in real space is not. Bots, or computer programs, can scan the Web and find content that the bot author wants to flag. The bot author can then collect links to that content and follow through however it seems most sensible.

Consider the story of fans of The Simpsons who find themselves summoned to court when their Simpsons fan pages are discovered by a bot hired by the television network Fox. The fans are not allowed, Fox said, to collect friends and strangers around these images of Bart Simpson and his dad. These images are "owned" by Fox, and Fox has the right to exercise perfect control. Though "[t]he sites are the Internet equivalent of taping posters of favorite actors to a bedroom wall," they are not permitted by copyright law.

Fan sites are not the only examples here. Dunkin' Donuts used the threat of a copyright lawsuit to force a site devoted to criticism of the nationwide chain to sell the site to the company. The company claimed it could "more effectively capture the comments and inquiries" if it owned the site. Maybe, but it is also certainly true that it could more effectively edit the content the site made public.

A more telling example is the history of OLGA—an on-line guitar archive started by James Bender at the University of Nevada, Las Vegas. As the Web site describes it:

OLGA is a library of files that show you how to play songs on guitar. The files come from other Internet guitar enthusiasts like yourself, who took the time to write down chords or tablature and send them to the archive or to the newsgroups rec.music.makers.guitar.tablature and alt.guitar.tab. Since they come from amateur contributors, the files vary greatly in
quality, but they should all give you somewhere to start in trying to play your favorite tunes.8

In 1996, the University of Nevada, Las Vegas, was contacted by EMI Publishing, which alleged that the site violated EMI’s copyright. The university shut the site down. The then-current archivist, Cathal Woods, moved the archive to another host. Then in 1998, OLGA was contacted again, this time by the Harry Fox Agency, which, like EMI, complained of copyright violations without specifying precisely what was being infringed. OLGA closed the archive in that year and then began a long (and as yet unresolved) campaign to establish the right of hobbyists to exchange chord sequences.

The pattern here is extremely common. Copyright holders vaguely allege copyright violations; a hosting site, fearing liability and seeking safe harbor, immediately shuts down the site. The examples could be multiplied thousands of times over, and only then would you begin to have a sense of the regime of control that is slowly emerging over content posted by ordinary individuals in cyberspace. Yahoo!, MSN, and AOL have whole departments devoted to the task of taking down “copyrighted” content from any Web site, however popular, simply because the copyright holder demands it.9 Machines find this content; ISPs are ordered to remove it; fearing liability, and encouraged by a federal law that gives them immunity if they remove the content quickly,10 they move quickly to take down the content.

This is the second side of the effect that cyberspace will have on copyright. Copyright interests obsess about the ability for content to be “stolen”; but we must also keep in view the potential for use to be more perfectly controlled. And the pattern so far has tracked that potential. Increasingly, as activity that would be permitted in real space (either because the law protects it or because the costs of tracking it are too high) moves to cyberspace, control over that activity has increased.

This is not a picture of copyrights imperfectly protected; this is a picture of copyright control out of control. As millions move their life to cyberspace, the power of copyright owners to monitor and police the use of “their” content only increases. This increase, in turn, benefits the copyright holders, but with what benefit to society and with what cost to ordinary users? Is it progress if every use must be licensed? If control is maximized?
CPHack

There's lots of junk on the World Wide Web. And there's lots that's worse than junk. Some of the stuff, for some people, is offensive or worse. The worse includes material deemed obscene or, and this is a very different category, "harmful to minors"—aka pornography.

As I've described, there's a long and tedious history of Congress's efforts to regulate porn in cyberspace. I'm not interested in that story here. I'm interested here in the efforts of companies to regulate porn in cyberspace by producing code that filters content.

The code I mean is referred to affectionately as "censorware." Censorware is a class of technology intended to block access to Internet content by forbidding a Web browser to link to the blocked sites. Censorware companies make it their job to skim the Web looking for content that is objectionable, and they then add the link to that content to their list. Their list of banned books is then sold to parents who want to protect their kids.

There is obviously nothing wrong with parents exercising judgment over what their kids get to see. And obviously, if the choice is no Internet or a filtered Internet, it is better that kids have access to the Internet.

But this does not mean that censorware is untroubling. For often the sites blocked by censorware systems are themselves completely unobjectionable. Worse, sites often are blocked merely because they oppose the technology of censorware. In December 2000, free speech activists at the civil rights group Peacefire reported that a number of censorware systems had begun to block Web sites affiliated with Amnesty International. This is just the latest in an endless series of similar cases. They all point to a technology that is fundamentally at odds with the openness and free access of the original Net.

In 1999, Eddy Jansson of Sweden and Matthew Skala of Canada decided they wanted to test out one instance of censorware—a product called Cyber Patrol. They therefore wrote a program, CPHack, with which a user could disable Cyber Patrol and then see which sites Cyber Patrol banned. The code thus made it easier, for example, for a number of sites to complain about the censorious practices of Cyber Patrol.

The owner of Cyber Patrol was not happy about CPHack. So like most owners unhappy with what others do, it raced into federal court. In March, Mattel brought suit against the authors and Peacefire, demanding it stop distributing its code for liberating the CP list.

Its claim was copyright violation. These coders, Mattel argued, had
violated Mattel's copyright by reverse engineering the code for Cyber Patrol—contrary to the license under which Cyber Patrol was sold. Because their use of Cyber Patrol was unlicensed, it was illegal.

There is something very odd about the claim that Mattel was making. Copyright's core is to protect authors from the theft of others. It is to protect Mattel, in other words, from someone who would steal Cyber Patrol and use it without paying for the program. Copyright is not ordinarily aimed at protecting authors from criticism. It doesn't "promote progress" to forbid criticism of what has happened before. But this is exactly how the law was being used in this case. By claiming that a contract that was attached to the copyrighted code banned a user from criticizing the code, the law was being used to restrict criticism.

Within two weeks, Mattel had received a worldwide injunction against the distribution of CPHack. The injunction was not just against the authors of the program; it also extended to those who linked to the program's site or who merely posted the program. These secondary posters believed they had a fairly strong right to post the code for CPHack. The code stated it was "GPL'd," which meant that anyone was free to take it and post it as he wished. But all these "conspirators" (as the law had to call them to justify this extraordinary federal action) were now bound by this emergency injunction of a U.S. court. And Mattel then moved quickly to perfect and make permanent this force of law.

Yet here, cracks in the case began to show. First there was the problem of jurisdiction. The authors of CP Hack were not citizens of the United States, and their work was not done in the United States. Copyright law, in the main, is national. Just because these two people somewhere in the world did something that would constitute a violation of copyright law in the United States does not show they violated United States copyright law. But even if there had been jurisdiction, there was a much more fundamental flaw. What exactly was the wrong that these defendants were said to have committed? Mattel said they had "reverse engineered" Cyber Patrol. Reverse engineering is ordinarily a permissible "fair use" under copyright law—copyright law has no incentive to make it impossibly difficult for others to compete with software programs. But, Mattel said, the license that Cyber Patrol was sold under did not give the purchasers any right to reverse engineer. Indeed, it expressly waived the right of the purchaser to reverse engineer the product.

The contract Mattel was speaking of was the sort of shrink-wrapped license that comes with most software today. When you install Cyber Patrol,
you are said to have agreed with everything on that license. Now whether such a license in general is enforceable is a hard question. The strongest case in the United States supporting its enforcement is a decision by Judge Frank Easterbrook in the Seventh Circuit Court of Appeals. But Easterbrook is clear that the restrictions beyond copyright law depend upon there being a contract. As he said, "Someone who found a copy of [a copyrighted work] on the street would not be affected by the shrink-wrap license—though the federal copyright laws of their own force would limit the finder's ability to copy or transmit the application program." Thus, to demonstrate that the authors violated the law, you would have to demonstrate they had purchased the product in a way that would have made them liable under the contract.

All that was going to be very hard to prove. But just at the moment the case was to come to trial, Mattel had a surprise. It had purchased the rights to CPHack from the original authors, and now it was simply enforcing the rights it was purchasing. No one, Mattel said, was free to distribute this code, because this code was now Mattel's.

There was a squabble at this point about whether in fact the code was Mattel's. The code had been distributed in a form that indicated it was governed by the GPL. The GPL made it impossible to sell the product in a way that would revoke that license—at least to those down the chain of distribution. The original sellers—who received nothing except the promise that this gaggle of American lawyers would go home—were quick then to deny that they had released the program under the GPL. But that denial rang hollow. The Mattel lawyers had apparently informed them that if Mattel had been tricked, they would be guilty of fraud. And while that would have been an idle threat (at least if the authors had simply agreed to transfer whatever rights they had), it was apparently threat enough to get the authors to deny that CPHack was in fact under the GPL.

Armed with this purchase, Mattel was able to convert the temporary injunction into something permanent. And the judge forbade others who had apparently been restricted by the injunction from intervening to challenge the injunction. As the case settled, and was affirmed by a court of appeals in Boston, Mattel had the rights to CPHack; no one else could distribute it, even if the purpose was simply to criticize the company, Mattel.

The first two centuries of copyright's history were two centuries of censorship. Copyright was the censor's tool: the only things that could be printed were those things printed by authorized presses; the only authorized presses were those cooperating with the Crown.
Here history has repeated itself, though the protected is not the Crown, but commerce. The law has become a tool for effectively disabling the ability of others to criticize a corporation. Coders can release code that censors the Net, and efforts to release the list of censors are censored by the law.

DeCSS

The lawyers for Mattel relied directly upon copyright law. But there was another tack they might have taken—one that will prove much more important as time goes on.

In 1998, Congress passed the Digital Millennium Copyright Act (DMCA). That act strengthened copyright in a number of ways, but one way was particularly troubling: This was its “anticircumvention” provision.

The anticircumvention provision regulates code that cracks code that is intended to protect copyrighted material. There are two parts to the provision—one that restricts the cracking of code that protects copyrighted material, and one that forbids the creation of code that cracks code that protects copyrighted material. In both cases, the aim of the law is to lend legal support to the tools that copyright holders deploy to protect their copyrighted material.

In the ordinary case—with ordinary property—there can be little in this to complain about. It is a crime to steal my car. But obviously, that isn’t enough to stop car theft. So many people install a burglar alarm in their car to further inhibit car theft. But obviously again, that too isn’t enough. So if a legislature, wanting to reduce the risk of theft even more, passes a law that makes it a crime to disable burglar alarms, or to sell tools whose sole purpose is to disable burglar alarms, there can’t be any complaint about these rules, either. If it is wrong to steal a car, and permissible for people to protect their property, it is wrong to crack technology designed to protect the property.

But this story about real property doesn’t map directly onto intellectual property. For as I have described, intellectual property is a balanced form of property protection. I don’t have the right to fair use of your car; I do have the right to fair use of your book. Your right to your car is perpetual; your right to a copyright is for a limited term. The law protecting my copyright protects it in a more limited way than the law protecting my car.

This limitation is not just laziness on the part of Congress. The limits on the law’s power to protect copyright are inherent in the clause granting Congress power to regulate copyright, and in the First Amendment’s restrictions on Congress’s power. Copyright law, for example, cannot protect
ideas; it can protect only expression. The law's protection can extend only for limited times. And fair use of copyrighted works is understood to be constitutionally required.

These limitations distinguish copyright as property from ordinary property. And that distinction suggests the trouble with direct analogy from laws protecting burglar alarms to laws protecting code protecting copyrighted work. If copyright law must protect fair use—meaning the law cannot protect copyrighted material without leaving space for fair use—then laws protecting code protecting copyrighted material should also leave room for fair use. You can't do indirectly (protect fair-use-denying-code protecting copyright) what you can't do directly (protect copyright without protecting fair use).

I am not arguing that it is illegal or somehow unconstitutional for individuals to deploy code that protects copyrighted material more than the law does. There are troubles with this, and I don't think the law can ignore them. But there is ordinarily no constitutional problem unless the law has actually done something.

But in the case I've described, the law has done something. The anticircumvention provision is law that protects code that protects copyrighted material. And my claim is simply that that law must be subject to the same limitations that a law protecting copyrighted material directly is.

How does all this relate to Mattel?

Well, Mattel released a product that was copyrighted. Arguably, at least, its compilation of sites is copyrighted. It protected this copyrighted material using code. This code is what CPHack hacked. Thus, arguably, CPHack violated the anticircumvention provision of the DMCA.

Mattel didn't bring this case, though I wish it had. Had it claimed the anticircumvention provision protected it, then the courts would have had a clear shot at the question of whether or not there are constitutional limitations on the power of Congress to protect code protecting copyright. The Cyber Patrol case would have been a perfect case to raise that claim. If cracking code to demonstrate that the code is censoring speech isn't fair use, then I'm not sure what would be.

Instead, this question of fair use was raised in a very different case.

In 1994, Hollywood started releasing movies on DVD disks. These movies were extremely high fidelity and relatively compact. The disks fit in an ordinary CD-ROM-size drive. And very quickly, manufacturers started producing drives that would read DVD disks.

To protect the movies on these disks, the industry developed an encryp-
tion system. This system was named CSS—Content Scramble System. CSS would make it difficult for a user to play back DVD content unless the user was using a machine that could properly decode the CSS routines.

The machines were DVD players that had been licensed to decrypt CSS-encrypted content. These licenses were issued by the consortium that developed and deployed CSS. And they were granted initially to companies that produced Windows- and Macintosh-compatible machines. Those running Windows, or those using a Mac, could play DVD movies on their machines.

Let's be clear first about what CSS did. CSS was not like those early software protection systems. It didn't interfere with the ability to copy DVD disks. If you wanted to pirate a DVD disk, all you needed to do was copy the contents from one disk to another. There was no need to decrypt the system in order to copy it.

So CSS didn't disable copying. All it did was limit the range of machines that DVD disks could be played on. And that in turn was the limitation that gave rise to the need for a crack.

For—surprise, surprise!—Macintosh and Windows are not the only operating systems out there. In addition, there are Linux PCs, among others. These machines could not play DVD movies. And owners of these machines were not happy about this limitation. So a number of them decided to develop a program that would crack CSS, so that DVDs could be played on other machines. And when open source coders developed such a program, they called it DeCSS.

DeCSS disabled the encryption system on a DVD disk. It turned out that CSS itself was a terribly poor encryption technology. And once the system had been cracked, it became possible to play DVD content on other computers. With DeCSS, DVD disks could be played on any machine.

Now again, DeCSS didn't make it any easier to copy DVDs than before. There's no reason you can't simply copy a CSS-protected movie and ship it to your friends. All that CSS did was ensure that you played the movie on a properly licensed machine. Thus, DeCSS didn't increase the likelihood of piracy. All that DeCSS did was (1) reveal how bad an existing encryption system was; and (2) enable disks presumptively legally purchased to be played on Linux (and other) computers.

But upon the release of DeCSS, the industry went nuts. Within six weeks, four lawsuits had been filed in four separate jurisdictions, seeking under many legal theories the quashing of this code. Within three weeks of the filing of the suits, two injunctions had been entered against people who
posted DeCSS code and even against journalists who linked to DeCSS.\textsuperscript{22} Once again, as with CPHack, the legal system had been fired up to silence this dangerous code.

The core case here was tried in New York. The defendants were many. Some had linked to the sites carrying DeCSS. Others had written articles about the sites and had linked to the links. And others were active distributors of DeCSS. None of these defendants was in the business of selling pirated movies. And at no time in the case did the plaintiffs demonstrate that any movies had been pirated because of DeCSS.

Instead, the sole claim in the case was that these defendants were in the business of distributing code that cracked an encryption system, and hence, these defendants were in violation of the anticircumvention provisions of the DMCA.

The district court judge in the New York case issued an immediate injunction stopping the distribution of DeCSS. After a long trial, he issued an opinion making permanent that injunction. The opinion making the injunction permanent rejected the argument that “fair use” entitled the defendants to produce or distribute this code. Fair use, the court concluded, was something copyright law must allow. This was a law regulating code, not a copyright. The court concluded that Congress had the power to allow private actors to pile on protection on top of the copyright law. No First Amendment interests were violated.

This case was appealed to the circuit court. At the time of this writing, that appeal has not been resolved. But the importance of the case is not how it ends; the importance is the signal that Hollywood sends: any system that threatens its control will be threatened with an army of Hollywood lawyers.

\textit{iCraveTV}

\textit{iCraveTV} was a site that streamed television content over the Internet.\textsuperscript{23} The site was located in Canada, where Canadian broadcasting law made such streaming legal. Under Canadian law, anyone has the right to rebroadcast television content, as long as he doesn’t change the content in any way. \textit{iCraveTV} wanted to take advantage of that right to give computer users access to TV.

The problem was that though TV was free in Canada, it was not free in the United States. To rebroadcast content in the United States requires the
permission of the original broadcaster. So behavior legal in Canada would be illegal in the United States.

But then where was iCraveTV? In one obvious sense, it was in Canada. But when it made itself available on the Internet, it was also, simultaneously, everywhere. That has been the character of the Internet since its birth—to be on the site at any place is to be on the site in every place.

iCraveTV took some steps to limit itself to one place. It tried to block non-Canadians from the site. But when it began this process, the technologies for blocking were not strong. iCraveTV asked for a telephone number, but of course it had no easy way to verify that the telephone number you gave it was your telephone number.

Soon after iCraveTV went on-line, copyright holders in the United States brought suit to shut it down. The theory? By setting up an Internet service to broadcast TV, iCraveTV was broadcasting TV into the United States. It was therefore violating U.S. copyright law (by “publicly performing” what iCraveTV streamed to American viewers). Until it could “guarantee,” as the Hollywood lawyers put it, that no United States citizen would get access to this free Canadian TV, the Canadian site had to be shut down.

There was a significant dispute about how hard iCraveTV was working to keep non-Canadians out of its site. The Hollywood lawyers hired Harvard Law School Berkman Center’s boy genius Ben Edelman to demonstrate just how easy it was to hack the iCraveTV site. But whether easy or not, the significant issue about the case is this: How much should someone in one country have to be burdened by the laws of another country?

For example: Imagine the Chinese government telling the American site China Online that it must shut down until it is able to block out all Chinese citizens, since the content on China Online is illegal in China. Or imagine a German court telling Amazon.com that it must stop its selling of Mein Kampf until it can guarantee that no German citizen will be able to get access to that book—since that book is illegal in Germany. Or imagine a French court telling Yahoo! that it has to block French citizens from purchasing Nazi paraphernalia, since that is illegal in France. (Oops, no need to imagine. A French court did just this.25)

In all these cases, we are likely to think that the action of these foreign governments is somehow illicit. That the free exchange of the Net tilts us in favor of open and regular access. That steps to shut down foreign sites because of local laws are the very essence of what the Internet was designed to avoid.
But when it comes to copyright law, we become like the Chinese, or Germans, or French. With respect to law, we too want to insist upon local control—especially because local law here is so strong. So with respect to copyright law, we push local control. And the result is the birth of technologies that will facilitate better local control.

iCraveTV, for example, promised the court that it would develop technology to make it possible to block out everyone except Canadians. Jack Goldsmith and Alan Sykes have described the growing collection of technologies that will achieve the same end. These suggest that the future will be very much like the past: life on the future Internet will be regulated locally, just as life before the Internet was regulated locally.

How we will get to that future world was one point of Code and Other Laws of Cyberspace. But for now, the significance of iCraveTV is again the attitude it evinces. Though there was no proof that any revenue would be lost by virtue of people streaming content through their TV, and though Canadian law was assumed to protect this behavior in Canada, the control industry raced to court to shut down the alternative. The courts complied.

**MP3**

In Chapter 8, I told the story of MyMP3—an innovative new service whose users could “beam” the content of their CD collection to a Web site and then get access to their music at that Web site. This service was provided by the company MP3.com. To provide access to this music, MP3.com had to purchase a very large collection of CDs. It then copied those CDs into its computer database. When a user of MyMP3 placed a CD into the Beam-it program, the system identified whether that CD was in MP3.com’s library. If it was, then that user account got access to the content of that CD whenever he or she accessed the account.

Ten days after launching the service, MP3.com received a letter from RIAA attorneys. Its service was a “blatant” violation of copyright laws, said the letter, and MP3.com should take the service down immediately. MP3.com refused, and the lawyers did what lawyers do when someone refuses: they filed suit in U.S. district court, asking for over $100 million in damages.

The RIAA lawyers had a point, if you looked at the statute quite literally. MP3.com may have purchased a bunch of CDs, but it had clearly “copied” these CDs when it created its single, massive database. There was, on its
face, then, an unauthorized copy of each of these CDs, and the question became whether or not this copy was nonetheless fair use.

Applying the ordinary standard for fair use, the RIAA argued that it was clearly not. This was for a commercial purpose. Thus, fair use was not a defense, and the blatant and willful copying was then a prosecutable offense.

When lawyers have such a clean, slam-dunk case, they get very, very sure of themselves. And the papers in the My.MP3 case are filled with outrage and certainty.

But when you stand back from the outrage and ask, “What’s really going on here?”, this case looks a lot different. First, as should be clear, My.MP3 was not facilitating the theft of any music. You had to insert a real CD into your computer before you could get access to the copy on MP3.com’s server. Of course, you could borrow someone else’s CD and hence trick the system into thinking you were the rightful owner of the CD. But you could borrow someone else’s CD and copy it anyway. The existing system permits theft; My.MP3 didn’t add to that.

Second, it should be fairly clear that this service would increase the value of any given CD. Using this technology, a consumer could listen to his or her CD in many different places. Once the system recognized your rights to the music on the CD, the system gave you those rights whenever you were at a browser. That means that the same piece of plastic is now more valuable. That increase in value should only increase the number of CDs that are purchased. And that increase would benefit the sellers of CDs.

Third, it is also fairly clear that exactly the sort of thing that MP3.com was doing could easily have been done by the consumers themselves. Any number of companies have created free disk space on the Internet. Anyone could “rip” his or her CDs and then post them to this site. This ripped content could then be downloaded from any computer. And this download could be “streamed” to be just like the service MP3.com was providing.

The difference is simply that users don’t have to upload their CDs. On a slow connection, that could take hours; on a fast connection, it still can be quite tedious. And a second difference is that the duplication that would be necessary for everyone to have his or her CDs on-line would be much less. Ironically, by shutting down MP3.com, the RIAA was inducing the production of many more copies of the very same music.

Thus the battle here was between two ways of viewing the law—one very strict and formal and the other much more sensitive to the consequences of one outcome over the other. And the claim of MP3.com was simply that the
court should consider the facts in the case before it shut down this innovative structure for distributing content. MP3.com was arguing for a right to “space-shift” content, so that a user’s content could be accessible anywhere.

But the court had no patience for MP3.com’s innovation. In a stunning decision, the court not only found MP3.com guilty of copyright violation, it also found the violation “willful.” And rather than giving nominal or minimal damages for this violation, the court imposed $110 million in damages. For experimenting with a different way to give consumers access to their data, MP3.com was severely punished.

Napster

I described the technology that is Napster in chapter 8. The essence was this: Napster enables individuals to identify and transfer music from other individuals. It enables peers, that is, to get music from peers. It does this not through a completely peer-to-peer architecture—there is a centralized database of who has what, and who, at any particular moment, is on-line. But the effect is peer-to-peer. Once the service identifies that X has the song that Y wants, it transfers control to the clients of X and Y, and these clients oversee the transfer. The Napster server has just made the link.30

But that was enough in the eyes of the recording industry. And with predictably lightning speed, it filed suit here as well. Napster was just a system for stealing copyrighted material. It should, the RIAA demanded, be shut down.

Against the background of MP3.com, Napster does look a bit dicey. After all, the service at issue in MP3.com was a service to give individuals access to content that they presumptively had purchased. On Napster, the presumption is the opposite. There seems little reason for me to download music I already own.

But even that is not quite correct. I’ve been a Napster user, though I am not an imaginative user, and I am generally quite lazy. I know exactly what I want to hear, and I know that because I own the music already. But it is easier simply to download and play the music I own on Napster than it is for me to go through the CDs I own (most of which are at home, anyway) and insert the one I want in a player. Thus, while I won’t say that none of the music I have listened to on Napster is music I don’t own, probably only 5 percent is.

That the user owned the music, however, didn’t stop the court in the
MP3.com case. And the assurance that users were only downloading music they already owned was not likely to satisfy the RIAA. Most people, the RIAA argued, used Napster's technology to "steal" copyrighted work. It was a technology designed to enable stealing; it should be banned like burglar's tools.

Copyright law is not new to a technology said to be designed solely to facilitate theft. Think of the VCR. The VCR records content from television sets. It is designed to record content from television sets. The designers could well have chosen to disable the record button when the input was from a TV. They could, that is, have permitted recording when the input was from a camera and not a TV. But instead, they designed it so that television content could be copied for free.

No one in the television industry gave individuals the right to copy television content. The television industry instead insisted that copying television content was a crime. The industry launched a massive legal action against producers of VCRs, claiming that it was a technology designed to enable stealing and that it should be banned like burglar's tools. As Motion Picture Association of America president Jack Valenti testified, the VCR was the "Boston Strangler" of the American film industry.31

This legal campaign ended up in the courtroom of Judge Warren Ferguson.32 After "three years of litigation, five weeks of trial and careful consideration of extensive briefing by both sides,"33 the trial court judge found that the use of VCRs should be considered "fair use" under the copyright act. The court of appeals quickly reversed, but the important work had been done in the trial court. The judge had listened to the facts. Sony was permitted weeks of testimony to demonstrate that, in fact, the VCR would not harm the industry. Sony was permitted, in other words, to show how this technology should be influenced by the law.

These findings were critical in the appellate review of the case. And when the case finally reached the Supreme Court, it gave the Supreme Court sufficient ground to understand matters in a balanced and reasonable way. Though the VCR was designed to steal, the Court concluded that it could not be banned as an infringing technology unless there was no "potential" for a "substantial noninfringing use."

Potential. For a substantial noninfringing use. Notice what this standard does not say. It does not require that a majority of the uses of the technology be noninfringing. It requires only that a "substantial" portion be noninfringing. And it does not require that this noninfringement be proven today. It requires only that there be a potential for this noninfringing use. As long
as one can demonstrate how the technology could be used in a way that was legitimate, the technology would not be banned by a court.

The Supreme Court’s test is rightly permissive. The tradition of American law is not to ban technologies, but to punish infringing use. And that test should have had an obvious answer in the context of the Napster case. Here there are no doubt lots of infringing uses. But there are also lots that under any fair estimation constitute fair or noninfringing use. Music that has been released to the Net to be freely distributed is freely distributed through Napster. That use is clearly noninfringing and is substantial. Music that has fallen into the public domain is available on Napster. That use is clearly noninfringing, and is substantial. And lots of recordings that are not music — lectures, for example — can be made available on Napster. The Electronic Frontier Foundation has a series of lectures that are traded on Napster; they are offered as content that is free.

But when this claim was made to Judge Marilyn Hall Patel in California, she, unlike Judge Ferguson in the Sony case, had no patience for the argument. Without a trial, and with barely contained contempt, she ordered the site shut down.

Within thirty-six hours, Napster attorney David Boies had received a stay of that order from the Ninth Circuit Court of Appeals. And after hearing arguments in the case, that court affirmed much in the injunction of Judge Patel. The court did, however, make one important modification: Napster was not responsible for contributory infringement unless the copyright holder made Napster aware of the violation. Napster therefore wasn’t closed down by the court; it wasn’t required to become the copyright police. But it was required to remove music posted contrary to the copyright holder’s wish. So, like the circuits of the computer Hal in the movie 2001, the music in the memory of the Napster system will be slowly turned off, as copyright holders will demand the right to control the sharing of their content.

Eldred

RECALL THE story of Eric Eldred’s HTML book library from chapter 8. As I described there, Eldred has a passion for producing HTML books from public domain works. As the Framers of our Constitution plainly envisioned, after a limited time, copyrights expire, and the work previously protected then falls into the public’s hands without restraint. Eldred takes those public domain works and turns them into freely accessible on-line texts.

But in recent years, Congress has changed the rules. In 1998, Congress
extended the term of existing copyrights by twenty years. As I've said, this was simply the latest extension in a pattern that began forty years ago. While Congress changed the term of copyright just once in the first hundred years of copyright, and once again in the next fifty years, it has extended the term of subsisting copyrights eleven times in the past forty years.

This latest extension meant that works that were to fall into the public domain in 1999 would now not be “free” until the year 2019. Thus, works that Eldred had prepared to be released were now bottled up for another generation.

This latest change outraged many, and especially Eric Eldred. Eldred threatened civil disobedience—promising to publish a series of Robert Frost poems that would have fallen into the public domain. After some of us convinced him that that was a very dangerous strategy, Eldred chose instead to challenge the statute in court. In January 1999, in a federal court in Washington, D.C., Eldred filed his complaint.

Eldred's claims were simple. If the Constitution permits Congress to grant authors an exclusive right “for limited times,” then the Framers of that power clearly intended that that exclusive right must come to an end. Permitting Congress the power to perpetually extend copyrights would defeat the purpose of the express limitation.

This was Eldred's claim based on the language of the copyright clause of the Constitution. He also raised an argument based on the First Amendment. The First Amendment says that Congress “shall make no law ... abridging the freedom of speech, or of the press.” Copyright is a law that certainly limits Eric Eldred's HTML press. So how are these two provisions of the Constitution—one granting Congress the power to issue copyrights, and the other limiting Congress's power to “abridge” the freedom of the press—to be reconciled?

The Supreme Court has explained how the two coexist. Copyright, the Court has written, is an “engine of free expression.” Because of the incentives that copyright law provides, work gets created that otherwise would not have been produced. This means that copyright law both increases speech and restricts it. And a fairly balanced copyright law can, in principle, at least, increase more than it restricts. That means that copyright law does not necessarily “abridge” speech; and hence the copyright clause does not necessarily conflict with the guarantees of the First Amendment.

But as Eldred argued, this rationale cannot justify extending the terms for existing copyrights. Existing copyrights protect work that is already created; extending the terms for this work restricts speech without any promise of fu-
ture creativity. The one thing we know about incentives, Eldred argued, is that incentives are prospective. Whatever we promise Hawthorne, he isn’t going to produce any more work.

Both claims appealed to the Framers’ sense of balance in establishing the copyright power. As Justice Joseph Story described it, the power gave authors exclusive control for a “short interval”; after that interval, the work was to fall into the public’s hands “without restraint.” At the time Story wrote that, a “short interval” was an initial term of fourteen years. Today, that “short interval” can easily reach ten times that term.

The courts, however, had little patience for the Framers’ sense of balance. Both the District Court and the Court of Appeals for the D.C. Circuit held that the copyright clause did not constrain Congress to a single “limited time.” It was free to grant extensions, as long as the extensions themselves were limited. (As Professor Peter Jaszi described it, Congress is therefore free to grant a perpetual term “on the installment plan.”) And more dramatically, in rejecting the First Amendment claim, the court of appeals held that “copyrights are categorically immune from First Amendment scrutiny.”

The meaning of these two holdings together is that the ability to propertize culture in America is essentially unlimited by the Constitution—even though the plain text of the Constitution speaks volumes against such expansive control. And the consequence of this power to propertize was perhaps best exemplified by a lawsuit to stop the publication of what many considered a sequel to Margaret Mitchell’s Gone with the Wind.

Gone with the Wind was published in 1936. Under the law as it existed then, Mitchell’s copyright would have expired at the end of 1992. But because of the extensions that Eldred was fighting, that copyright now extends until 2031. Until then (or later, if Congress extends the term again), the Mitchell estate has exclusive rights over the story, as well as over other stories that are sufficiently close to the original to be called “derivative.”

In 2001, Alice Randall tried to publish a work called The Wind Done Gone. While she called it a parody of Gone with the Wind, that was her lawyers speaking more than Randall. The work is clearly based on Mitchell’s work; in telling the story of Gone with the Wind from the perspective of the African slaves, it clearly relies upon Mitchell’s work in an intimate and extensive manner. The Mitchell estate called the work a sequel and brought a federal lawsuit to stop its publication. This story, the Mitchell estate essentially argued, was theirs to control well into the twenty-first century.
To most people, this is plainly absurd. Gone with the Wind is an extraordinarily important part of American culture; at some point, the story should be free for others to take and criticize in whatever way they want. It should be free, that is, not only for the academic, who would certainly be allowed to quote the book in a critical essay; it should be free as well for authors like Alice Randall as well as film directors or playwrights to adapt or attack as they wish. That's the meaning of a free society, and whatever compromise on that freedom copyright law creates, at some point that compromise should end.

The Gone with the Wind case, as well as Eldred's case, is still working its way through the courts. But both tell a similar story: The freedom to build upon and create new works is increasingly, and almost perpetually, restricted under existing law. To a degree unimaginable by the Framers of our Constitution, that control has been concentrated in the hands of the holders of copyrights—increasingly, large media companies.

CONSEQUENCES OF CONTROL

the Internet in its nature shocks real-space law. That's often great; it is sometimes awful. The question policy makers must face is how to respond to this shock.

Courts are policy makers, and they too must ask how best to respond. Should they respond by intervening immediately to remedy the "wrong" said to exist? Or should they wait to allow the system to mature and to see just what harm there is?

In the context of porn, as I have already argued, the courts' response is to wait and see. And indeed, this is the response of the government in many different contexts. Porn, privacy, taxation: in each case, courts and the government have insisted we should wait to see how the network develops.

In the context of copyright, the response has been different. Pushed by an army of high-powered lawyers, greased with piles of money from PACs, Congress and the courts have jumped into action to defend the old against the new. They have legislated, and litigated, quickly to assure that control of the old is not completely undermined by the new.

Ordinary people might find these priorities a bit odd. After all, the recording industry continues to grow at an astounding rate. Annual CD sales have tripled in the past ten years. Yet the law races to support the recording industry, without any showing of harm. (Indeed, possibly the opposite: when
Napster usage fell after the court restricted access, album sales fell as well. Napster may indeed have helped sales rather than hurt them.40

At the same time, it can’t be denied that the Net has reduced the ability that parents have to protect their children. Yet the law says, “Wait and see, let’s make sure we don’t harm the growth of the Net.” In one case—where the harm is the least—the law is most active; and in the other—where the harm is most pronounced—the law stands back.

Indeed, the contrast is even stronger than this, and it is this that gets to the heart of the matter.

The Internet exposes much more copyrighted content to theft than in the world that existed before the Internet. This much of the content holders’ claim is plainly true.

But as I’ve argued, the Internet does two other things as well. First, the Internet makes it possible (if the proper code is deployed) to control the use of copyrighted material much more fully than in the world before the Internet. And second, the Internet opens up a range of technologies for production and distribution that threaten the existing concentrations of media power.

In responding to the shock that the Internet presents to copyright law, it is of course important to account for the increased exposure to theft. But the law must also draw a balance to assure that this proper response to an increased risk of theft does not simultaneously erase the important range of access and use rights traditionally protected under copyright law. If the Net creates an initial imbalance, the response by Congress should not create an equal and opposite imbalance, where traditional rights are lost in the name of perfect control by content holders.

That was my argument in Code. But now we should add a second concern to that same story: The response by Congress should also not be such as to permit this concentrated industry of today to leverage its control from the old world into the new. Artists deserve compensation. But their right to compensation should not translate into the industry’s right to control how innovation in a new industry should develop.

Control, however, is precisely Hollywood’s and the recording labels’ objective. In the context of copyright law, the industry has been very clear: Its aim, as RIAA president Hilary Rosen has described it, is to assure that no venture capitalist invests in a start-up that aims to distribute content unless that start-up has the approval of the recording industry.41 This industry thus demands the right to veto new innovation, and it invokes the law to support its veto right.42
Michael Robertson of MP3.com agrees that this is the aim and effect. "[T]his litigation," Robertson told me, "is as much about straddling the competition as anything else." And it has had its effect.

What they've done very successfully is dried up the capital markets for any digital music company. [W]e went public a little over a year ago [and] raise[d] $400 million from going public. Today, if you took a digital music company business plan, you couldn't get a buck and a half from a venture capital company.

This is the reality that the current law has produced. In the name of protecting original copyright holders against the loss of income they never expected, we have established a regime where the future will be as the copyright industry permits. This puny part of the American economy has grabbed a veto on how creative distribution will occur.

One could quibble about whether current law is properly interpreted to give existing interests this control. Some see these cases (in particular the MP3.com and Napster cases) as simple; I find them very hard. But whether they are simple or hard, the underlying law is not unchangeable. Congress could play a role in making sure that the power of the old does not trump innovation in the new. It could, that is, intervene to strike a balance between the right of copyright holders to be compensated and the right of innovators to innovate.

The model for this intervention is something we've already seen: the compulsory license. For recall, as I described in chapter 4, the first real Napster-type case: cable television. It, like Napster, made its money by "stealing" the content of others. Congress in remedying this theft required that the cable companies pay content holders compensation. But at the same time, Congress gave cable television companies the right to license broadcasting content, whether or not the copyright holder wanted to.

Congress's aim in part was to assure that the cable industry could develop free of the influence of the broadcasters. The broadcasters were a powerful industry; Congress felt (rightly) that cable would grow more quickly and innovate more broadly if it was not beholden to the power of broadcasters. So Congress cut any dependency that the cable industry might have, by assuring it could get access to content without yielding control.

Compensation without control. The same solution is available today. But the recording industry is doing everything it can to keep Congress far from this solution. For it knows that
if it has the absolute right to veto distribution that it can't control, then it can strike deals with companies offering distribution that won't threaten the labels' power. The courts, whether rightly or not, have handed the labels this veto power; Congress, if it weren't flustered by the emotion of the recording industry, could well intervene to strike a very different balance.

We find that balance by looking for a balance—not by giving copyright interests a veto over how new technologies will develop. We discover what best serves both interests by allowing experimentation and alternatives.

But this is not how the law is treating copyright interests just now. Instead, they are in effect getting more control over copyright in cyberspace than they had in real space, even though the need for more control is less clear. We are locking down the content layer and handing over the keys to Hollywood.

The costs of this lockdown are great enough without the Internet; the Internet makes them much more significant. Before the Internet, as I described in chapter 7, production was concentrated in the hands of the few. With the Internet, this production could be widespread. But to the extent that content remains controlled, to the extent the Alice Randalls or Eric Eldreds must seek permission to use or build upon other aspects of our culture, these controls create barriers to new creativity. They block the potential for innovation, by adding protections for existing interests.

Okay, time for a politics check. I know what you're thinking: These are just the ravings of a rampant leftist. But as writer Siva Vaidhyanathan argues, "There is no 'left' or 'right' in debates over copyright. There are those who favor 'thick' protection and those who prefer 'thin.'" The argument in favor of balance is not a liberal vs. conservative argument. The argument is old vs. new.

The credentials of at least some conservatives in this debate cannot be questioned. Circuit judge Richard Posner—father of much in law and economics, and perhaps the most prolific and influential judge of the last hundred years—has written persuasively about the complexity in finding balance in copyright law. As I've described, the property right of copyright is incomplete. As Posner writes:

Since the property right is incomplete, one might suppose that literature is being underproduced and therefore copyright protection should be ex-
panded in both scope and duration—perhaps made comprehensive and perpetual. The matter is not so simple.\textsuperscript{49}

Not simple—indeed, quite complex. The complexity is just what we've been considering throughout this book. Intellectual property is both an input and an output in the creative process; increasing the "costs" of intellectual property thus increases both the cost of production and the incentives to produce. Which side outweighs the other can't be known a priori. "An expansion of copyright protection," Posner argues, "might . . . reduce the output of literature . . . by increasing the royalty expense of writers."\textsuperscript{50} Thus the ideal mix cannot be found simply by increasing the power of copyright holders to control.

Other conservatives are a bit more colorful about the point. Consider, for example, one of the brightest stars of the Ninth Circuit Court of Appeals, Judge Alex Kozinski.

Kozinski is an immigrant. His family suffered at the hands of Romanian communism; they fled Romania when he was twelve.\textsuperscript{51} In 1985, he was appointed by President Reagan to the federal bench. He has since then been the darling of the Federalist Right. He is an extraordinarily talented and insightful judge, who has little patience for the paternalism of the liberal Left.

But the extremes of copyright drive him mad, and there is no better an opinion describing his view of limited copyright terms than a dissent he wrote to an opinion upholding the right of Vanna White to control the use of images that would remind the public of her.

At issue in the Vanna White case was whether intellectual property law—in particular, a state-created right of publicity—would permit Vanna White of Wheel of Fortune fame to control all images that suggest her, including in this case any advertisement that "evokes the celebrity's image in the public's mind."\textsuperscript{52}

The Court of Appeals for the Ninth Circuit—or, as that circuit includes California, the Court of Appeals for the Hollywood Circuit, as Kozinski puts it\textsuperscript{53}—upheld White's right to control the use of this image. Kozinski sharply dissented. As he wrote:

Something very dangerous is going on here. Private property, including intellectual property, is essential to our way of life. It provides an incentive for investment and innovation; it stimulates the flourishing of our culture; it protects the moral entitlements of people to the fruits of their labors. But reducing too much to private property can be bad medicine.\textsuperscript{54}
Why? For the same reasons we've been tracking throughout this book.

Private land... is far more useful if separated from other private land by public streets, roads and highways. Public parks, utility rights-of-way and sewers reduce the amount of land in private hands, but vastly enhance the value of the property that remains.55

The state must therefore find a balance, and this balance will be struck between overly strong and overly weak protection.

Overprotecting intellectual property is as harmful as underprotecting it. Creativity is impossible without a rich public domain.56

But is that unfair? Is it unfair that someone gets to profit off the ideas of someone else? Says Kozinski, No.

Intellectual property law assures authors the right to their original expression, but encourages others to build freely on the ideas that underlie it. This result is neither unfair nor unfortunate: It is the means by which intellectual property law advances the progress of science and art. We give authors certain exclusive rights, but in exchange we get a richer public domain.57

This balance reflects something important about this kind of creativity: that it is always building on something else.

Nothing today, likely nothing since we tamed fire, is genuinely new: Culture, like science and technology, grows by accretion, each new creator building on the works of those who came before. Overprotection stifles the very creative forces it's supposed to nurture.58

This balance is necessary, Kozinski insists, "to maintain a free environment in which creative genius can flourish."59 Not because "flourish[ing]" innovation is the darling of the Left, but because innovation and creativity were the ideals of our founding republic.

MY STORY so far has been about copyright and, indirectly, its cousin, trademark law.60 I have argued that these two bodies of rights will together be
used by the old to protect themselves against the threat of the new. This protection is not necessary; there is nothing in our tradition that compels it. But it is pushed not by those with the most to lose, but by those without the most to win. And I have argued that we should be skeptical about just this sort of protectionism.

But now I want to describe a second form of protectionism—perhaps more threatening to the promise of the Internet’s future. This threat too is the product of state intervention into Internet space. And this intervention is even harder to justify.\[61\]

The issue here is patent law.\[62\] A patent is a form of governmental regulation. It is a state-backed monopoly granting exclusive rights to an “inventor” for an invention deemed useful, novel, and nonobvious.

The argument favoring patents is as old as the hills. If an inventor can’t get a patent, then he will have less incentive to invent. Without a patent, his idea could simply be taken. If his idea could simply be taken, then others could benefit from his invention without the cost. They could, in other words, free-ride off the work of the inventor. If people could so easily free-ride, fewer would be inventors. And if fewer were inventors, then we would have less progress in “science and useful arts.”

Getting more progress is the constitutional aim of patents. So the question that must always be asked of any patent regime is whether we have good reason to believe that patents have that effect. As Harvard law professor Stephen Shavell has written, “there is no necessity to marry the incentive to innovate to conferral of monopoly power in innovations.”\[63\] So is there any evidence that it does any good?

In some cases, the evidence is good.\[64\] For some kinds of innovations, patents are extremely likely to induce more innovation. In particular, in theory, where innovation is independent, or noncumulative (meaning one invention is essentially separate from another), then economists predict that patents will clearly benefit innovation.\[65\] Likewise, even where innovation is cumulative, if the use of the patent is clear, then in principle, the original patent holder will have a strong incentive to license a patent to follow-on innovators.\[66\] But here, economists have an important qualification: If we don’t know which direction an improvement is likely to take, then licensing may not occur, and patents here may actually do harm.\[67\] Thus, for economists, at least, the theory suggests contexts in which innovation will be helped by patents as well as contexts where it will be harmed.\[68\]
The empirical evidence is less encouraging. The strongest conclusion one can draw is that whatever benefit patents provide (except in industries such as pharmaceuticals), it is small. As economist Adam Jaffe concludes, "[T]he value of patent rights might still be too small relative to overall costs and returns to have a measurable impact on innovative behavior." And as he concludes more broadly:

There is a widespread unease that the costs of stronger patent protection may exceed the benefits. Both theoretical and, to a lesser extent, empirical research suggest this possibility. Economists have long understood that, at a theoretical level, technological competition can lead to a socially excessive level of resources devoted to innovation. The empirical literature is convincing that, for the research process itself, the externalities are clearly positive on balance (Griliches, 1992). But to the extent that firms' attention and resources are, at the margin, diverted from innovation itself towards the acquisition, defense and assertion against others of property rights, the social return to the endeavor as a whole is likely to fall.

Other commentators increasingly agree. As The Economist recently summarized a broad range of research: "Do firms become more innovative when they increase their patenting activity? Studies of the most patent-conscious business of all—the semiconductor industry—suggest they do not." This skepticism has been with us from the start of the patent system. Ben Franklin thought patents immoral. Some of the greatest inventors of our history have refused to patent most of their inventions. Science has traditionally resented patents. And even Bill Gates, no patry when it comes to intellectual property protections, expressed skepticism about software patents. As he wrote in a memo to Microsoft executives in 1991:

If people had understood how patents would be granted when most of today's ideas were invented and had taken out patents, the industry would be at a complete standstill today.

The first patent commissioner himself—Thomas Jefferson—was also extremely skeptical about these forms of monopoly. Commenting upon the proposed Constitution, with its proposed provision for granting monopolies to cover writings and inventions, Jefferson wrote that he wished the draft would be amended to eliminate any monopolies. As he wrote:
I sincerely rejoice at the acceptance of our new constitution by nine states. It is a good canvas, on which some strokes only want retouching. What these are, I think are sufficiently manifested by the general voice from north to south which calls for a bill of rights. It seems pretty generally understood that this should go to juries, habeas corpus, standing armies, printing, religion and monopolies. . . . The saying there shall be no monopolies lessens the incitement to ingenuity, which is spurred on by the hope of a monopoly for a limited time, as of 14 years; but the benefit even of limited monopolies is too doubtful to be opposed to that of their general suppression. 78

Jefferson's views about patents were not his alone. From the beginning of the Supreme Court's interpretation of the law of patent, it has affirmed that patents are no natural right; that the scope of patent rights is just as far as Congress extends it. And Congress should extend it only when Congress has reason to believe the monopolies it extends will do some good.

In the first two hundred-plus years after Congress first enacted a patent statute, the duration and scope of patent law were fairly stable. The Framers set a term of four years; they quickly extended that to fourteen; and that term is close to the current term of twenty. And from the start, patents were not granted for just anything; invention was required. So too today, when an invention must be novel, nonobvious, and useful. 79

But in the past twenty years, an important shift has occurred. The limits to the reach of patent law have been eroded by a number of expansions in patent law doctrine. "These changes," Adam Jaffe writes, "were not brought about primarily by Congressional action, but rather by the . . . Patent Office." 80

The expansions I want to focus on here are those relating to cyberspace. And these include the patenting of software inventions and business methods.

Before the 1980s, software inventions in the United States were not subject to patent protection. The reasons were tied to the nature of programming (programs were considered algorithms, and algorithms were traditionally not protected), but the arguments in favor of not making software patentable were more pragmatic. Since software is often distributed without its source, it is often extremely hard to understand how it is in fact achieving its effect. On the surface, functions could be implemented in any number
of ways. When you sort a list of addresses within an address book program, in principle, the algorithm that sorts the list could be one of a million such programs. (There's more than one way to skin a cat.) When you display a picture, how the picture is displayed is nothing that is obvious to the developer or user.

But beginning in the 1980s, courts started recognizing software inventions as patentable inventions. And by the early 1990s, these patents had taken off. Patent applications for software-related patents went from 250 in 1980 to 21,000 in 1999, and the number granted has increased eight- or ninefold.81

What was most striking about this explosion of law regulating innovation was that the putative beneficiaries of this regulation—coders—were fairly uniformly against it. As Richard Stallman put it, "We did not ask for the change that was imposed upon us."82 And this attitude was not limited to free software advocates. When the U.S. Patent Office began explaining this new benefit it would be providing software developers, key developers from a range of software industries were frantic in avoiding the benefit. As Douglas Brotz from Adobe Corporation said in 1994:

I believe that software per se should not be allowed patent protection. I take this position as the creator of software and as the beneficiary of the rewards that innovative software can bring in the marketplace. . . . [Adobe and I] take this position because it is the best policy for maintaining a healthy software industry, where innovation can prosper.83

Oracle took the same position.84 The system wasn't broke, these coders said. It certainly didn't need Washington to fix it.

But Washington was not to be deterred, and the push for software patents did not go away. Quite the opposite. Over time, the push was for even broader patent protection—this time to cover business processes as well as software inventions.

A software-implemented business process patent is a patent for a process of doing business, sufficiently novel and nonobvious to earn the U.S. Patent and Trademark Office's favor.85 Most thought such processes beyond the reach of patent law. This was not because patent law never covered processes—it plainly did. But the expectation was that it would not cover business processes because adequate return from the process itself would create a sufficient incentive to invent.86

In 1998, however, the United States Court of Appeals for the Federal Cir-
cuit put this idea to rest. The patent law reached business processes just as any other, and patents for business methods were, the court held, not invalid because of the subject matter.87

The case in which this issue arose was one where a financial services company had developed a new kind of mutual fund service, one that would manage a pool of mutual funds through a software-based technology. The court upheld both the software patent and the patent on the business method. Both, the court said, were inventions that the patent law could reach. This decision, in turn, gave birth to an explosion of business method patent applications. And by 1999, many were beginning to be approved in a way that surprised the industry. Applications for computer-related business methods jumped from about 1,000 in 1997 to over 2,500 in 1999.88 High on that list was the Amazon 1-Click patent, but also on the list were Price-line.com’s reverse auction patent, and British Telecom’s claim that it owned the invention of hypertext links (and hence the World Wide Web!).89

In all these cases, the question the monopoly-granting body asked was simply this: Was this sort of “invention” sufficiently like others that were the subject of patents? If so, then the patent was granted for this field of innovation.

Economists, however, are likely to ask a much different question. While it is clear that patents spur innovation in many important fields, it is also clear that for some fields of innovation, patents may do more harm than good.90 While increasing the incentives to innovate, patents also increase the costs of innovation. And when the costs outweigh the benefits, patents make little sense.

How could this be? The answer links to an argument we’ve seen in many different contexts before. The ordinary argument for a strong patent right is a kind of prospecting theory. First advanced by Edward Kitch, the prospect theory says there is good reason to hand out broad, strong patents because then others will know with whom they should negotiate if they want to build upon a certain innovation.91 This in turn will create incentives for people to invent, and as information is a by-product of invention, it will induce “progress” in the “useful arts.”92

The problem with this theory, however, is its very strong assumption (in some contexts, at least) that the parties will know enough to properly license the initial foundational invention, or that other issues won’t muck up the incentives to license.93

Both limitations on the ability to license are what economists would call transaction costs.94 The transaction cost from ignorance is similar to the in-
sight the founders of the Net had when they embraced an end-to-end architecture: rather than architecting a system of control from which changes could be negotiated, they were driven by humility to a system of noncontrol to induce many others to experiment with ways of using the technology that the experts wouldn't get.95

The transaction cost affecting incentives to license is in part a problem of ignorance, but in part the problem of strategic behavior that we've seen in many different contexts. It is the problem Christensen is discussing in *The Innovator's Dilemma*: the problem of nonneutral platforms that guided my review in chapter 4 of open code projects.

My claim is not that these transaction costs are so high as to make patents unadvisable in the Internet context. My point is simply that these considerations, supported as they have been,96 at least raise a question.

So given this complexity, you might think that policy makers would be eager to know whether the fields covered by software and business method patents are the sorts where innovation is helped by patents or harmed. You might think—given the extraordinary importance that these markets have played in the recent economic boom—that before the government tries to fix something through monopolies, it would check to see if anything is broken.

I had the chance to ask the government just this. In a debate in Washington, I was on a panel with Q. Todd Dickinson, patent commissioner in the last days of the Clinton administration. In my part of the opening presentation, I suggested that it would be important to know whether patents will help in these fields or harm.

Dickinson was impatient with the suggestion. As he said:

Some days I wish I was the professor and only had to think about these things and not do the work. But I got an office to run. And I've got 1,500 applications coming in this year and I have to figure out what to do with them. I don't have the luxury to wait for five years for Congress to figure out whether they will change the law or not.

Publisher and Net guru Tim O'Reilly was on the same panel. He had a quick and devastating response. The head of the U.S. Patent Office, O'Reilly said, has two roles in the administration. One is, as Dickinson had just said, to run the office. But the other is to advise the administration about what policy made sense. And where, O'Reilly asked, following up on my
own question, was the policy analysis that justified this extraordinary change in regulation?

I remember thinking, Where are the Republicans when you need them? Here was critical new regulation that would significantly affect innovation in cyberspace. Here was the regulatory impact statement? Here was a government official overseeing a radical expansion in patent regulation, within a field that had been the most important component of growth in the United States' economy in the past twenty years. Yet the government didn't have time to learn whether its patent policy would do any harm or good? Regulate first, ask questions later.

There's good reason to wonder whether patents are necessary in a field such as this. Patent law is designed to create a barrier against idea theft, so that inventors have an incentive to invent and use their ideas. The term of this protection is not to be overly long; patents are monopolies; monopolies raise prices. The term should be long enough to give enough incentive, without being so long as to raise prices unnecessarily.

But a patent isn't the only device that might protect the innovator against inefficient copying. Being first to market in a network economy creates a first-mover advantage without imposing the costs of a patent.

And other incentives are often sufficient to induce innovation without a patent. Jeff Bezos, for example, said of the 1-Click patent that Amazon.com would have developed the 1-Click technology whether or not there was a patent system. The reason is obvious: The system helps sell more books, and the profit from those additional sales of books is enough of an incentive for the invention of new technology.

Either one of these reasons, plus a host of others suggested by legal and economic scholars, would lead a rational policy maker to ask whether monopoly is needed here. But this question has not been asked about patents affecting cyberspace.

so why is Washington doing it? What reason could there be for the government to allow this launch of regulation to occur without even a hearing about whether the regulation will do any good?99

The answer is obscure, but we can identify a number of causes. First is the patent bar itself. Dickinson is not an evil man; his heart is certainly in the right place. But he is a political figure, who feels the pressure of the interest group that is most affected by the decisions of his department. That
interest group is the patent bar—a group of lawyers who like a world where their market increases dramatically. What interest do they have asking whether this increased regulation does any good?

Second is our general way of thinking about patents. Most of us don’t think about patents as a form of regulation. Most consider patents property in the same sense that my car is property. In that same debate, patent king Jay Walker was also on the panel. He argued that the question in this debate about patents was whether you were for property or against it—and in his view, the pro-property view was "beyond reproach."100

But again, this is just silly. Patents are no more (and no less) “property” than welfare is property. Granting patents may make sense, as providing welfare certainly makes sense. But the idea that there is a right to a patent is just absurd. From the very beginning, our tradition has self-consciously understood that the only question guiding whether to issue a patent or not is whether or not patents will do society any good. As conservative economist Friedrich von Hayek put it:

> It seems to me beyond doubt that in [the fields of patent and copyright] a slavish application of the concept of property as it has been developed for material things has done a great deal to foster the growth of monopoly and that here drastic reforms may be required if competition is to be made to work.101

Rather than reason, what governs the current patent debate is bias—bias in favor of a system that seems right just because it seems old.102 But the relevant system is not old—it is being expanded in ways that would shock lawyers of a generation ago. And something is right not because it is old, but only if it does some good. But we will never know whether or not it does any good if we accept this never-ending expansion without limit. We will never know what benefit this regulation provides until we begin to demand that the regulation prove itself.

For the harms from this regulation are not hard to identify, and for the cynical, or conspiratorial, the harms are not surprising. (On the margin, the costs of a patent system will harm small inventors more than large; negotiating a patent system is easier for IBM than for the garage inventor.)103 And the harms from an expanded American patent system will harm foreign inventors more than American. (It is easier to hire American law firms locally than from a distance.) Thus this expansion in patent protection will shift the
competitive field away from the small, non-American inventor in favor of the large, American inventor.104

The harms are even more pronounced, however, for open code projects. Tim Berners-Lee has noticed its effect on Web development already. ("Developers are stalling their efforts in a given direction when they hear rumors that some company may have a patent that may involve the technology."105 One example is the development of P3P, which may enable better protection of privacy on the Web.) And open code proponents—like software developers generally—have been among the strongest opponents to patents in this field. As Richard Stallman writes, "The worst threat we face comes from software patents, which can put... features off-limits to free software for up to twenty years."106 Red Hat chairman Bob Young thinks much the same: "[S]oftware patents are an evil, or at least [a] very damaging encroachment on the efficacy of the software programming industry."107

The reason patents harm open code in particular is not hard to see. Think about the mechanics of licensing a patent when you are licensing for anyone working on an open code project. Who knows who they are? How many users need to be sanctioned? As Peter Wayner writes, "[T]hese questions are much easier to answer if you're a corporation charging customers to buy a product."108 Thus patents tilt the process to harm open code developers.

The problem is exacerbated with software patents because though the patent system was designed to induce inventors to reveal their invention to the public, there is no obligation that a software inventor reveal his source code to get a patent. "The single most revealing symptom" of the failure of the existing system, Professor Brian Kahin writes, "is that the software professionals do not read patents."109 As Bob Young analogizes it, "It's like that ceramic guy, producing a new kind of ceramic and [patenting it] without ever telling anyone how he made the extra hard ceramic. So in software you're saying 'I'm patenting software that has this look and feel, but I don't actually have to tell people how I achieved that look and feel.' The source code remains a secret."110

And then there is the expense of patents, which is borne more sharply by smaller inventors than larger. The costs include the costs of securing a patent, but those in the end are trivial. The real costs are borne by those who would challenge a patent. If the U.S. Patent Office makes a mistake, and a patent is granted that shouldn't be granted, then it costs on average $1.5 million (for each side) to take a patent dispute to trial.111
Finally, there is the obvious “hold-up” problem—where an innovator is about to release a product and is discovered to be violating a patent. As Berkeley economist Carl Shapiro describes it:

The hold-up problem is worst in industries where hundreds if not thousands of patents, some already issued, others pending, can potentially read on a given product. In these industries, the danger that a manufacturer will “step on a land mine” is all too real. The result will be that some companies avoid the minefield altogether, i.e., refrain from introducing certain products for fear of hold-up. Other companies will lose their corporate legs, i.e., will be forced to pay royalties on patents that they could easily have invented around at an earlier stage, had they merely been aware that such a patent either existed or was pending.\(^{112}\)

As Shapiro concludes, “[T]his ‘hold-up’ problem is very real today, and . . . should [be considered] a problem of first-order significance in the years ahead.”\(^{113}\)

This may be an unintended consequence of this recent expansion in protection. I am, for example, quite certain this would not have motivated the different courts that have contributed to this expansion. But it may well explain why there is little passion from those who fund lobbyists to find a way to cut back on the expansion. By letting things go as they are, this change may well give them a competitive advantage over the innovator who can’t fund a legal team or isn’t from the United States. Again, as Bill Gates of Microsoft told his senior management:

A future start-up with no patents of its own will be forced to pay whatever price the giants choose to impose. That price might be high: Established companies have an interest in excluding future competitors.\(^{114}\)

This story about the potential danger of patents in a field where innovation is sequential and complementary (where one builds on another, and the second complements the value of the first) gets additional support from an ingenious argument that Michigan law professor Michael Heller initially made and that economist James Buchanan has now followed up on.\(^{115}\) Heller introduces the concept of an “anticommons.” If a commons is a resource where everyone has a right to use the resource (and therefore sometimes overuse the resource), an anticommons is a resource where many have the right to block the use of a resource by others (and therefore many
more underuse the resource). Heller gives the example of formerly state-owned buildings in post-Soviet Russia: Because of the many claims that could be made on them, the buildings were never developed. Too many bureaucrats could veto any project, and thus insufficient effort at innovating in the use of these buildings was made.

Nobel Prize-winning economist James Buchanan has expanded this idea to the problem of regulation generally. He points to the problem of patents in particular as an example where multiple and overlapping patent protection may create an anticommons, where innovators are afraid to innovate in a field because too many people have the right to veto the use of a particular resource or idea. This potential for strategic behavior by these many rights holders makes it irrational for an innovator to develop a particular idea, just as the possibility of veto by many bureaucrats may leave a particular piece of real property underdeveloped.

These ideas map directly onto the argument we’ve considered in this book. Control, when complex, can often increase the costs of using a resource; increasing those costs can easily chill innovation. Recall the extreme of AT&T’s control over innovation in the telecommunications system: Who would waste his or her time developing for that system, when any development would require convincing so many quasi bureaucrats before it could even be tried?

The complexity in these rights to exclude creates this anticommons problem. And the more severe the problem, the more it will stifle new innovation.

I’ve told a story about intellectual property in two critical competitive contexts. In both contexts, the emerging regime will have a significant regulatory effect. In both contexts, the regime will shift protection from the new to the old. The law in both cases will, on the margin, protect the old against the new. RIAA president Hilary Rosen was clear about this objective in the context of copyright law: No new ideas should be allowed unless the old system of distribution okays it. And this will be the certain, if unintended, consequence of the patent system as well. Those most likely to be displaced by new innovation will have the power, through these government-backed monopolies, to check or inhibit this innovation.

This power is the product of government-backed monopolies that in the ordinary case raise little trouble. I am not against copyright law (I agree with Hollywood: if you have simply copied the whole of this book, you are a thief); in the ordinary case, the scope of its monopoly ought to be respected.
But when we, as a society, undergo a radical technological shift—which the Internet revolution certainly is—then we should reexamine the scope of the monopoly power we extend and ask once again whether that power makes any sense. Is it necessary? Is there reason to believe it will do some good?

The tradition before the Internet had favored massive increase in the scope of copyright law and a significant increase in the reach of patents. Essentially anything you could attribute to a creative work, you had to respect by getting the permission of this creative work before using it.

In a world like the world I described as the dark ages, this may not be a terrible thing. When all publishers are largeish corporations, who really cares if creative energies must be licensed? The licensing process is an ordinary cost of doing business, just like paying sales tax or filing statements with the SEC. It may, on the margin, inhibit a bit, but not a terribly significant amount.

But when the world of creativity shifts outside the largeish corporation—when individuals and smaller groups are much more enabled to do this creative activity—then this system of exclusive licenses for every derivative use of a creative work begins to tax the creative process significantly. The opportunity cost, as economists would describe it, of this system of control is higher when, without this system of control, much more creative activity would go on.

Thus, when we have a massive shift in opportunity, we should be reevaluating how necessary these systems of control are. We should be asking whether control is necessary, or at least how far control is required. And if we don’t have a good reason for extending these systems of government-backed control, then we shouldn’t. If we have no good reason to believe a government-backed monopoly will help, then we have no good reason to establish government-backed monopolies.

At the end of chapter 7, I argued that the control of media in the dark ages may well be a product of economic constraints. That as long as economics constrains, then this system of concentration and control may be inevitable. The constraints I identified are not to be imagined or ignored away. They are real and unavoidable.

But the constraints that I have described in this chapter are different. They are not "real" in the same sense. The constraints of IP are constraints we build. We create regimes of IP, and then the regimes we have built yield the control I have identified. No doubt these regimes are in large measure
justified. No doubt in the main they promote progress. But often (in copyright for sure, and possibly with patents as well) the regime expands beyond its initial justification. The restrictions it imposes are artificial, in the sense that they don't promote progress; they simply benefit one person at the expense of another.

This then presses the fundamental question of this book: If the extremes of these constraints are not necessary, if there is no good showing that they do any good, if they limit the range of creativity by virtue of the system of control they erect, why do we have them?

For this is a change. The content layer—the ability to use content and ideas—is closing. It is closing without a clear showing of the benefit this closing will provide and with a fairly clear showing of the harms it will impose. Like the closing of the code layer described in chapter 10, this closing of the content layer is control without any showing of a return. Mindless locking up of resources that spur innovation. Control without reason.

This closing will not be without cost. Making it harder for innovations to enter, making resources more universally controlled—this will drive new competitors off the field, leaving the field once again safe for the old.

And more important, this closing does not occur without a purpose. As I suggested at the end of the last chapter, our greatest fear should be of dinosaurs stopping evolution. More precisely, we should be most concerned when existing interests use the legal system to protect themselves against innovation that might threaten them. The commitment of a society open to innovation must be to let the old die young. The law should resist becoming a tool to defend against the new; when change is on the horizon, it should allow the market to bring about that change.

This is just what is not happening in the field of intellectual property. The state is being pushed to defend expanded intellectual property rights in the name of protecting the way the world was.

As in chapter 10, we are allowing an idea about “property” to overrun the balance that grants access. Because we don't see that balance, or don't see the place for balance, we are quick to follow the arguments that favor control.

Again, this idea in the background—the sanctity of perfect control—blinds us. We in turn render blind the opportunities for innovation. When the only innovation that will be allowed is what Hollywood permits, we will not see innovation. That lesson, at least, we have already seen.