Imagine that a bustling group of colonists has just moved into a new area, a huge, unexplored plain. (Again, assume the native inhabitants have conveniently disappeared.) Some of the colonists want to farm just as they always did in the old country. “Good fences make good neighbors” is their motto. Others, inspired by the wide-open spaces around them, declare that this new land needs new ways. They want to let their cattle roam as they will; their slogan is “Protect the open range.” In practice, the eventual result is a mixture of the two regimes. Fields under cultivation can be walled off but there is a right of passage through the farmers’ lands for all who want it, so long as no damage is done. This means travelers do not need to make costly and inefficient detours around each farm. In the long run, these “public roads” actually increase the value of the private property through which they pass. They also let the ranchers move their cattle around from one area of pasture to another. The ranchers become strong proponents of “public, open highways” (though some people muse darkly that they do very well out of that rule). Still, most people want open highways; the system seems to work pretty well, in fact.
Two new technologies are introduced. First, the automobile is developed. Now thieves can drive through the farmers’ fields, stop quickly to grab some corn or a lettuce, and be back on the highway before they can be caught. Of course, the farmers’ costs have also fallen dramatically; now they have tractors to work their fields and trucks to take their products to distant markets. The farmers do not dwell on the benefits of the new technology, however. Understandably, they focus more on the profits they could reap if they could get all the advantages of the technology and none of its costs. They demand new legal protections aimed at producing that result. “What’s good for agriculture is good for the nation,” they say. But now comes the second technological shock—the development of barbed wire. The cost of erecting impassable barriers falls dramatically. The farmers begin to see the possibility of enclosing all of their land, roads and fields alike. This will help them protect their crops from pilfering, but it will also allow them to charge people for opening the gates in their fences—even the gates on public roads. That is a nice extra revenue stream which will, the farmers say, “help encourage agriculture.” After all, more fences mean more money for farmers, and more money for farmers means they can invest in new methods of farming, which will mean everyone is better off, right?

What is to be done? Assume that each side presents its case to the legislature. There are three obvious possibilities:

First, the legislature can simply tell each side to work it out amongst themselves. The law will continue to forbid trespass, but we are neither going to make it a crime to put up a barbed wire fence if it blocks legitimate public rights of way nor to make it a crime to cut a barbed wire fence, unless the fence cutter is also a trespasser. The farmers can attempt to enclose land by putting barbed wire around it. Ranchers and drivers can legally cut those fences when they are blocking public rights of way. Trespass remains trespass, nothing more.

Second, the legislature could heed the ranchers’ fears that barbed wire will permit the farmers not only to protect their own land, but to rob the public of its existing rights of way, turning open highways into toll roads. (The ranchers, of course, are more concerned with the rights of cattle than people, but most drivers agree with them.) As a result, the state could forbid the erection of a barbed wire fence where it might block a public right of way—classing it as a kind of theft, perhaps.

Third, the legislature could take the farmers’ side. Theorizing that this new automobile technology presents “a terrible threat to agriculture, because of
rampant crop piracy,” the state could go beyond the existing law of trespass and make it a crime to cut barbed wire fences wherever you find them (even if the fences are enclosing public lands as well as private, or blocking public roads). To back up its command, it could get into the technology regulation business—making the manufacture or possession of wire cutters illegal.

The state picks option three. Wire cutting becomes a crime, wire cutters are classed with lock picks and other “criminals’ tools,” and the people who make wire cutters are told their business is illegal. A storm of protest arises in the rural driving community. The wire cutter manufacturers claim that their products have lots of legitimate uses. All to no avail: the farmers press on. They have two new demands. Cars should be fitted with mandatory radio beacons and highways put under constant state surveillance in order to deter crop theft. In addition, car trunks should be redesigned so they can hold less—just in case the owner plans to load them up with purloined produce. Civil libertarians unite with car manufacturers to attack the plan. The farmers declare that the car manufacturers are only interested in making money from potential thieves and that the civil libertarians are Nervous Nellies: no one has anything to fear except the criminals. “What’s good for agriculture is good for the nation,” they announce again. As the barbed wire gates swing shut across the highways of the region, the legislature heads back into session.

BETWEEN PARANOIA AND REALITY: THE DMCA

I have argued that confusing intellectual property with physical property is dangerous. I stand by that argument. Yet analogies to physical property are powerful. It is inevitable that we attempt to explain new phenomena by comparing them to material with which we are more familiar. While the content companies’ tales of “theft” and “piracy” are the most prevalent, they are by no means the only such analogy one can make. In this chapter I try to prove that point.

The Farmers’ Tale is my allegorical attempt to explain the struggle over the single most controversial piece of intellectual property legislation in recent years, the Digital Millennium Copyright Act, or DMCA. The DMCA did many things, but for our purposes its crucial provisions are those forbidding the “circumvention of copyright protection systems,” the technological measures that copyright holders can use to deny access to their works or control our behavior once we get access. These measures include encryption, controls
on how many times a file can be copied, password protection, and so on. Copyright protection systems are, in other words, the digital equivalent of barbed wire, used to add an additional layer of “physical” protection to the property owner’s existing legal protection. But, unlike barbed wire, they can also control what we do once we get access to the property.

The rules that forbid circumvention of these systems are logically, if not elegantly, referred to as the anticircumvention provisions. They are to be found in Section 1201 of the Copyright Act, an ungainly and lumpily written portion of the law that was inserted in 1998 as part of the complex set of amendments collectively referred to as the DMCA. I will explain the significance of these rules in a moment. My hope is that the analogy to the Farmers’ Tale will make them a little easier to understand—at least for those of you for whom talk of digital rights management, anticircumvention provisions, and network effects is not second nature.

Notice the differences between this allegory and the “Internet Threat” storyline I described in the last chapter. There are two sets of bad guys in the Farmers’ Tale. The greedy thieves (who are still thieves in this story—not heroes) and the greedy farmers who use a genuine if indefinite “threat” posed by a new technology to mask a power grab. The Internet Threat is the story of an industry devastated by piracy, in desperate need of help from the state to protect its legitimate property interests. By contrast, the Farmers’ Tale is the story of a self-interested attempt not only to protect property but to cut off recognized rights of public access in a way that will actually make the whole society worse off. The legitimate role of the state in protecting private property has been stretched into an attempt to regulate technology so as to pick winners in the marketplace, enriching the farmers at the expense of consumers and other businesses. In the long run this will not be good for business as a whole. A patchwork of private toll roads is an economic nightmare.

That is not the most worrying part of the story: the farmers’ proposals are moving in the direction of regulating still more technology—the mandatory radio beacons and constantly monitored roads conjure up a police state—and all to protect a bunch of hysterical vegetable growers whose political clout far outweighs their actual economic importance.

Both the Internet Threat and the Farmers’ Tale are, of course, ways to understand what is currently going on in the intellectual property wars. In the digital realm, the part of the farmers is played by the content companies, the recording industry associations, the movie and software trade groups. Pointing to the threat of digital piracy, they demanded and received extra legal protection
for their copyrighted content. Unlike earlier expansions—longer copyright terms, more stringent penalties, the shrinking of exceptions and limitations, expansions in copyrightable subject matter—this was not a protection of the work itself; it was a protection of the digital fences wrapped around it, and a regulation of the technology that might threaten those fences.

What is the significance of this? The digital revolution makes it easier to copy copyrighted content. It also makes it easier to protect that content, and to do so in a more granular and precisely calibrated way. Imagine being able to sell a paperback book that could only be read by the original purchaser or a song that could only be listened to by a particular person in a particular room. Digital rights management technology makes it a lot easier to do these things. Suddenly the copyright owners have considerable physical control over their songs, e-books, and software, even after they have sold them. It is as if the recording industry or the publishers had a representative in your living room. They can use that control not merely to prevent illicit copying but to control and limit usage in ways that go far beyond their exclusive rights under copyright. All of this happens without the law or the state doing anything. Like barbed wire, this is a technological protection measure.

Like the farmers, the content companies were not content with their barbed wire alone. They wanted legally protected barbed wire in addition to their existing legal rights under copyright. Under the Digital Millennium Copyright Act, it became illegal to circumvent a technical protection measure such as encryption—the digital barbed wire behind which content companies secrete their work—even if what you did with the content when you got past the barbed wire was a fair use; excerpting a fragment of a film for a school presentation, for example, or making a copy of an encrypted audio file for personal use in another device. In other words, by using digital barbed wire, the content companies could prevent citizens from making the “fair uses” the copyright law allowed. This undermines some of the limitations on their exclusive rights that the Copyright Act explicitly carves out in Section 107, and thus shifts the balance of power that the Copyright Act establishes. Cutting barbed wire became a civil wrong, and perhaps a crime, even if the wire blocked a public road. Under most circumstances, making wire cutters was also now against the law.

The ranchers—whose digital equivalents are communications companies and hardware manufacturers—chafed under these new rules. The most powerful groups managed to get special dispensations. Internet service providers, for example, got a qualified immunity from copyright infringement that
occurs over their networks. But ordinary citizens, librarians, and civil libertarians also complained, and they were not as well represented in the legislature. It is true that the new rules may help to prevent illicit copying, but they also strike a blow against the exercise of fair use rights—rights that are important both to free speech and competition. Even if the content companies were absolutely right about the threats from digital piracy, this consequence should make us pause. But critics of the DMCA say that there is little evidence that the content companies are right. They quote some of the empirical studies I mentioned in the last chapter, particularly the ones that show no net negative effect from unauthorized music downloading on CD sales. They claim—and they are on strong ground here—that even if there are some losses from the new copying technologies, there are also benefits. Like the farmers, the critics would argue, the content companies take the benefits of the new technology for granted, but wish the law to step in to ameliorate the harms it also creates. And like the farmers, they are not yet satisfied. Their new proposals go even further—scarily further. Thus runs the critics’ argument.

The critics of the DMCA conjure up a world in which it will be illegal to lend each other books or songs, where it will be impossible for us to copy even small fragments of digital work for criticism or parody, where encryption research will be severely “chilled,” and where large quantities of the public domain will be enclosed together with the copyrighted content that the DMCA is supposed to protect. (The Electronic Frontier Foundation’s “Unintended Consequences” studies give concrete examples.)² They think the DMCA undoes the balance at the heart of copyright law, that it can be used to entrench existing businesses and their business methods, that it threatens speech, competition, privacy, and innovation itself. In short, they think the DMCA is the worst intellectual property law Congress has ever passed and view the adoption of similar laws around the world with a reaction little short of horror.

Those who supported the DMCA disagree, of course, and do so honestly. They see rampant piracy as a reality and the threat to fair use as some kind of academic hypothetical rarely encountered in reality. What’s more, many of them do not think fair use is that important economically or culturally. If markets work well, users could be made to pay for the rights that fair use gives—but only if they wanted them. One could buy expensive digital books which one was allowed to share, quote, or copy for classroom use, and cheaper ones which one had to keep to oneself. Remember that for many of the people who supported the DMCA, fair use is something of a “loophole”; certainly
not an affirmative right of the public or a reserved limitation on the original property grant from the state. (Remember the Sony Axiom from Chapter 4?) They find the analogy of fair use to a public road ludicrous. This film, or book, or song, is mine; anything you do with it, or to it, you do at my sufferance. (Remember the Jefferson Warning from Chapter 2?)

How has the DMCA worked in reality? Which group’s attitudes were vindicated? Two case studies may help us to answer these question.

Infectious Speech: The DMCA and Freedom of Expression

Jon Johansen, a 16-year-old Norwegian, was the unwitting catalyst for one of the most important cases interpreting the DMCA. He and two anonymous helpers wrote a program called DeCSS. Depending on whom you listen to, DeCSS is described either as a way of allowing people who use Linux or other open source operating systems to play DVDs on their computers, or as a tool for piracy that threatened the entire movie industry and violated the DMCA.

A little background is in order. When you play a commercial DVD, your actions are partly controlled by a simple encryption scheme called CSS, or the Content Scramble System. The DVD Copy Control Association licenses the keys to this encryption system to the manufacturers of DVD players. Without a key, most DVDs could not be played. The manufacturer then embeds this key in its hardware design in such a way that it is easy for your player to decode and play the movie but hard, at least for a person of average technical competence, to copy the decoded “stream.”

Because the DVD Copy Control Association will only license keys to manufacturers whose DVD players conform exactly to their specifications, the CSS scheme can also be used to control viewers in other ways. For example, DVD players are required to have one of six “region codes,” depending on where in the world they are sold. Region 1 is the United States and Canada. Region 2 is Japan, Europe, South Africa, the Middle East, and—bizarrely—Greenland. Region 3 is South Korea, Taiwan, and Hong Kong; and so on. The CSS scheme can be used to restrict a movie to a player with the appropriate region code. If you try to play a movie coded for region 6 (China) in a DVD player from region 1, it will not play. This allows filmmakers to distribute different versions of films to different regions at different times based on sequential release in cinemas, or simply to distribute DVDs with different prices to different regions without worrying about whether the cheaper DVDs will “leak” into the more lucrative markets. CSS and the hardware scheme that unlocks it can also...
be used to prevent you from fast-forwarding through the commercials at the beginning of the movie if the copyright owner does not want you to, or from skipping the FBI notice. The machine will not do it. In fact, it is deliberately built so that it cannot do it.

What we have here is a digital fence that is partly used to prevent copying. Movie studios are understandably worried about the worldwide circulation of perfect digital copies of their movies. CSS was supposed to help to prevent that, or at least make it much harder. But because almost all movies are encrypted with CSS and access to the keys comes with conditions, CSS also allows a more fine-grained control over consumers. Manufacturers are not allowed to make players which can view movies from all region codes or skip portions of the DVD that the owners do not want you to skip. The licensing body puts it this way on its Web site: “Q. Under the terms of the CSS licensing agreement, is it legal for a licensed manufacturer to produce and sell a product which allows a user to disable any CSS protections? A. No. Such products are not allowed under the terms of the CSS license. They are illegal.”

A technology introduced to protect intellectual property rights allows control in ways that those rights alone do not.

Before the DMCA, the movie companies could have done exactly this. They could have wrapped their movies in a digital fence. The consumer electronics companies that wanted to could license a key and be allowed to use a trademark that indicated that they were approved by the DVD Copy Control Association. But what if a manufacturer of DVD players felt that American consumers wanted to be able to play their Japanese anime movies without buying another DVD player to do so? Or what if they thought people were antsy and did not want to watch the FBI notice before every film? The manufacturer could have tried to “reverse engineer” the CSS system, to figure out how it worked. If they succeeded, they could make a player that was free of the restrictions that the CSS licensing authority imposed.

Of course there were some legal limitations even before the DMCA. Our hypothetical manufacturer could not break into the safe where the CSS code was being held or bribe an employee to provide it. (That would be a trespass or a violation of trade secret law.) It could not violate copyright laws over the various types of software that controlled DVD players. It could not use the trademarks of any of the entities involved, including any seal of approval granted by the DVD Copy Control Association. But it could—at least in the United States—try to reverse engineer the product so as to make a competing product with features that the customers liked more. It would be no more
illegal than a company making a cheaper generic razor cartridge that fits my expensive Gillette Mach 3 razor, a generic printer cartridge to replace the expensive one in my Lexmark printer, or, for that matter, a generic remote control for my garage door opener. In each case, of course, the original manufacturer would prefer that I use their products rather than the unlicensed ones. They can design their product to make it hard to use a generic replacement or even tell me that my warranty will be void if I use one. But they cannot say that the unlicensed product is illegal. We are back in option one of the Farmers’ Tale, before the legislature acted. The farmers can put up their wire, and even use it to block passage that would be otherwise legal, but it is not a crime to figure out a way through the fence unless the fence cutter is also a trespasser. The DMCA, however, might have changed all of that.

Let us return to Mr. Johansen, the 16-year-old Norwegian. He and his two anonymous collaborators claimed that they were affected by another limitation imposed by the CSS licensing body. At that time, there was no way to play DVDs on a computer running Linux, or any other free or open source operating system. (I will talk more about free and open source software later.) Let’s say you buy a laptop. A Sony Vaio running Windows, for example. It has a slot in the side for DVDs to slide in and software that comes along with it which allows the DVD reader to decode and play the disk. The people who wrote the software have been licensed by the DVD Copy Control Association and provided with a CSS key. But at the time Mr. Johansen set out to create DeCSS, the licensing body had not licensed keys to any free or open source software developers. Say Mr. Johansen buys the Sony Vaio, but with the Linux operating system on it instead of Windows. The computer is the same. The little slot is still there. Writing an open source program to control the DVD player is trivial. But without the CSS key, there is no way for the player to decode and play the movie. (The licensing authority later did license an open source player, perhaps because they realized its unavailability gave Mr. Johansen a strong defense, perhaps because they feared an antitrust suit, or perhaps because they just got around to it.)

Mr. Johansen and his supporters claimed strenuously that DeCSS was not in fact an aid to illicit copying. In fact, they argued that CSS was not really designed to protect DVDs against illicit copying. Commercial DVD “pirates” do not need to crack the CSS encryption. Quite the contrary: they produce exact copies of the DVD, CSS encryption and all, and the buyer’s player dutifully decodes it and plays it. Mr. Johansen claimed that his goals were very different from those of the pirates.
The motivation was being able to play DVDs the way we want to. I don’t like being forced to use a specific operating system or a specific player to watch movies (or listen to music). Nor do I like being forced to watch commercials. When your DVD player tells you “This operation is not allowed” when you try to skip commercials, it becomes pretty clear that DRM really stands for Digital Restrictions Management.4

In Mr. Johansen’s view, CSS was simply an attempt to control consumers, an attempt which should be a valid target for legal reverse engineering. He has a point. There were indeed other ways to copy DVDs which did not require DeCSS and which gave you files of more manageable size. CSS was indeed more than a simple anticopying device. The entire scheme—the keys, the licenses, the hardware requirements—was designed to give movie studios greater control over their movies in a number of ways, some of them unrelated to copying. On the other hand, he overstated the point. One function of CSS was indeed to make it harder for the average person playing a DVD on a computer to copy the file from the DVD to her hard disk and give it to a friend. It is very easy for the average 14-year-old to take a commercial music CD, change the songs into smaller files in the MP3 format, and share them with a friend. It is not as easy to do the same thing to a DVD—not impossible, just harder—and CSS is one of the reasons why.

Mr. Johansen’s program, DeCSS, was quickly made available worldwide. Mirror sites provided copies of the program and lists of such locations were easy to find using standard search tools. One such list was provided by the online site run by a magazine called 2600: The Hacker Quarterly. The magazine features everything from pictures of pay phones from around the world to tips on how to hack into computer or telephone systems. Its publisher is one Eric Corley, who goes by the name Emmanuel Goldstein—the resistance leader in George Orwell’s 1984.

In 1999, Universal City Studios brought suit against a number of individuals for distributing DeCSS. The case was called Universal City Studios v. Reimerdes et al. Corley was among the defendants. The suit prominently included a claim that the defendants were violating the DMCA. It was in this case that the DMCA received its first major legal challenge.

Depending on the characterization of the facts, the case seems to be about very different things. It could seem a classic First Amendment fight. (“Plucky magazine publisher told copyright law forbid him from linking to other sites on the Internet!”) Or it could seem the very essence of illegal activity. (“Shady site which unashamedly caters to computer ‘hackers’ tries to spread access to the burglar’s tools of cyberspace!”)
Of course, most lawsuits involve conflicts over facts. Much of what lawyers do is put the same facts into different conceptual boxes. But here, merely describing what Corley does, what hackers are, or what 2600 magazine is all about involves one in a profound culture clash. The best way to capture the clash may be to quote from an early entry about Corley in Wikipedia, the remarkable online encyclopedia.

The encyclopedia first quotes the description of 2600 magazine from Judge Lewis A. Kaplan, the federal district court judge who decided the Reimerdes case.

“2600: The Hacker Quarterly has included articles on such topics as how to steal an Internet domain name, how to write more secure ASP code, access other people’s e-mail, secure your Linux box, intercept cellular phone calls, how to put Linux on an Xbox, how to remove spyware, and break into the computer systems at Costco stores and Federal Express. One issue contains a guide to the federal criminal justice system for readers charged with computer hacking. In addition, 2600 operates a web site located at 2600.com (http://www.2600.com), which is managed primarily by Mr. Corley and has been in existence since 1995.”

The Wikipedia article then continues as follows:

While the judge’s tone is clearly disapproving, others would point out that bookstores, movies and television channels are filled with material on how to commit murder . . . and that without the efforts of the hacker community, however ill-intentioned, computer insecurity would be even more of a problem than it already is.\(^5\)

In fact, Judge Kaplan was not entirely disapproving. He mentions articles in 2600 that cover laudable or innocuous tasks, as well as others about tasks that most readers would find objectionable and rightly think to be illegal. But the anonymous volunteer who wrote this version of Corley’s Wikipedia entry clearly saw the issue differently. Wikipedia does not portray the hacker community as universally benevolent (“however ill-intentioned”), but that community is also seen as providing a useful service rather than merely a set of how-to guides for would-be digital burglars.

To most people, pointing out vulnerabilities in computer security systems seemed, at least in 1999, like telling the world that your neighbor has forgotten to lock his door and all his possessions are there for the taking. But to the online community, it is by no means so clear. From the perspective of those who are knowledgeable in the field, there is a moral continuum. There is clearly legitimate computer security and cryptography research, which includes
attempts to break into computer systems to test their defenses—that is how
one finds out they are secure, after all. Then there are “hackers.” This term
could be used to describe those who merely like to program. Richard Stallman,
for example, the originator of the free software movement, describes himself
thus. But the term could also be used for those who are interested in security or
interoperability—making two systems work together. That was Mr. Johansen’s
declared goal, after all. But some self-described hackers go further. They believe
that exploring and disclosing the weaknesses of supposedly secure systems is
intellectually fulfilling, practically important, and protected by the First
Amendment. They disclaim both moral and legal responsibility for the conse-
quences of their disclosures. (Or at least the negative consequences; they fre-
quently take credit for the positive consequences, such as improved security.)
Finally, there are “crackers,” whose interest in gaining entry to computer sys-
tems is malicious or for financial gain. At what point on this continuum does
the activity become legally, or morally, unacceptable? As the Reimerdes trial
went on, it became clear that the answer the DMCA gave might not be the
same as the one given even by undeniably legitimate computer scientists.

A large number of legal arguments were involved in the Reimerdes case, but
for our purposes here the most important ones dealt with the relationship be-
tween copyright and the First Amendment. What is that relationship?

In one obvious sense copyright actually aids free speech. By providing an
incentive to create works, copyright “add[s] the fuel of interest to the fire of
genius,” and thus helps to create the system of decentralized creative production
and distribution I described in Chapter 1. But copyright also restrains speech.
At its base, it allows an individual to call upon the state to prevent someone
from speaking or expressing themselves in a particular way. This may involve a
simple refusal to let the speaker use some text, picture, verse, or story in their
message, or it may involve a refusal to let them transform it in some way.

Neither copyright law nor the American Constitution is blind to these
dangers. Copyright has a number of built-in safeguards. The most important
of these is that copyright only covers “original expression”—both the ideas
and facts in this book can be used by anyone without my permission. Thus,
goes the theory, the speaker’s freedom of expression is never truly restrained.
The only thing I am barred from is using your words, your exact plot, your
photograph, your music—not your facts, your ideas, your genre, the events
you describe.

That is not always enough, of course. Sometimes the problem is that the
speaker cannot paraphrase around the restraints posed by copyright. He needs
to use the particular text or image in question to convey his message. The ideas, the facts, or a mere paraphrase of the expression would not be enough. In cases like that copyright’s answer is “fair use.” A politician could not prevent journalists who disagree with him from quoting his autobiography in discussing his life. If an African-American author wishes to tell the story of Gone With the Wind from the slaves’ perspective, she may do so in the face of the copyright holders’ attempts to stop her. Even fair use, though, may not cover every concern about free expression. Before World War II, Alan Cranston—later a U.S. Senator—wanted to convince American readers that the version of Hitler’s Mein Kampf published in the United States was distorted. He believed it to be slanted toward American sensibilities, downplaying both anti-Semitism and German expansionism. His solution? To publish his own English translation, taken direct and uncut from the German edition. He wanted to prove, with Hitler’s own words, that the United States had a dangerously distorted version of the German leader. But this is the kind of thing copyright law forbids and it is not clear that fair use allows. (In the end he did it anyway.7)

For the moment though, it is enough to realize that copyright law is not immune from the First Amendment or from free speech concerns more generally. If we do not notice that most of the time, it is because the internal limitations of copyright—fair use, the idea-expression distinction, and so on—generally take care of the First Amendment issue, not because the issue was never there.

So what First Amendment issues did the DMCA present? Most obviously, the DMCA gave a new right to copyright owners. By using a few simple technological measures, they could distribute a work in a particular format and yet, because of their new intellectual property right, they could make illegal an otherwise lawful process of gaining access for the purposes of making fair use. Of course, the First Amendment allows me to make fair use factually impossible. I can do that without raising any constitutional issues by hiding my manuscript and never letting you see it or just by using unbreakable encryption on my digital products. It allows me to use existing conventional property rights to make fair use illegal. If I own the only copy of the book and it is inside my house, it would be trespass for you to enter. No First Amendment problem there. But in passing the DMCA, Congress had created a new intellectual property right inside copyright law itself, a law aimed directly at expression, that made it illegal to get access for the purpose of making fair use even when you legally bought the physical book, or the physical DVD, and now wish to quote
it or parody it. Even that is not the problem. It is that Congress cannot grant the exclusive rights of copyright without simultaneously accompanying them by the limitations of fair use. Regardless of what physical constraints and tangible property rights might do to limit my ability to make fair uses, Congress had now, by law, allowed a copyright owner to distribute a particular work with the exclusive rights but without some of those limitations.

Imagine that Congress had passed the following law instead of the DMCA: “Any copyright owner can make it illegal to make a fair use of a copyrighted work by putting a red dot on their books, records, and films before selling them. It shall be a crime to circumvent the red dot even if, but for the dot, the use would have been fair.” That would be clearly unconstitutional. It gives copyright owners a new intellectual property right to “turn off fair use” in copyrighted works distributed to the mass market. Is the DMCA not the same thing?

This was the issue in Reimerdes. True, if I cut through the digital fence on a DVD in order to excerpt a small portion in a critical documentary, I would not be violating your copyright, but I would be violating the anticircumvention provisions. And DeCSS seemed to be a tool for doing what the DMCA forbids. By providing links to it, Mr. Corley and 2600 were “trafficking” in a technology that allows others to circumvent a technological protection measure. DeCSS could, of course, be used for purposes that did not violate copyright—to make the DVD play on a computer running Linux, for example. It enabled various noninfringing fair uses. It could also be used to aid illicit copying. But the alleged violation of the DMCA had nothing to do with that. The alleged violation of the DMCA was making the digital wire cutters available in the first place. So one First Amendment problem with the DMCA can be stated quite simply. It appeared to make it illegal to exercise at least some of the limitations and exceptions copyright law needs in order to pass First Amendment scrutiny. Or did it just make it very, very difficult to exercise those rights legally? I could, after all, make a videotape of the DVD playing on my television, and use that grainy, blurry image in my documentary criticizing the filmmaker. The DMCA would not be violated, though my movie might be painful to watch.

The other possible First Amendment problem with the DMCA was that in regulating programs such as DeCSS, the DMCA was actually regulating “speech.” The first challenge to the DMCA was that, by making tools like DeCSS illegal, the DMCA took away a constitutionally necessary escape hatch to copyright, thus making copyright law as a whole violate the First
Amendment’s guarantee of freedom of speech. The second challenge was different. The problem was that the program itself was speech and the DMCA was regulating it illicitly.

The reasoning went like this. A computer program is a form of expression and communication. The source code can even be read by human beings. True, it is an abstract form of communication—like musical notation and mathematical algorithms. But those are clearly protected by the First Amendment. Congress could not make Schoenberg’s twelve-tone scale illegal or punish mathematicians for physics equations that seemed to support a theory of the universe’s origin other than the creationism that is currently so popular. True, the source code is a description of a method of doing something, and the code can, if run on a computer, produce a result—but one could argue that those attributes do not affect the First Amendment’s protection. Neither a recipe for hash brownies nor a player piano roll for the Nazi “Horst Wessel” song could constitutionally be prohibited, even though actually to make the hash brownies would be illegal, and even though the piano roll is functional (it “makes” the player piano play the tune). True, most people cannot read computer code, but speech does not need to be common or accessible to be protected. In fact, the courts have even held that the choice to communicate in a particular language is constitutionally protected in some settings.

On the other hand, software code is undeniably functional. Lots of functional articles can be said to have some expressive content—a gun, an airbag, a crash helmet, a set of burglar’s tools, a computer virus. And many actions have expressive content: a terrorist bombing, for example. Surely these could be regulated by Congress? To the defendants, DeCSS looked like a physics equation, a musical score, or a recipe. To the movie studios, DeCSS had all the First Amendment significance of a crowbar, lock pick, or, for that matter, a car bombing. The same argument was repeated over the hyperlinks that Corley and others provided to sites which carried the DeCSS program. Speech or function? To the defendants, forbidding 2600 to link to these sites was like preventing the Washington Post from describing the availability of drugs on certain blocks of 16th Street. To the movie companies, the hyperlinks were the equivalent of loading potential buyers into a van, taking them down there, and giving them enough money to make the purchase.

Which of the two First Amendment arguments is more convincing? That the DMCA is a congressionally created off-switch for fair use? Or that software code is speech and the DMCA restricts it? Like a lot of scholars, before
Reimerdes went to trial, I thought that the first argument was by far the more powerful. I still do. I thought the odds of the court buying the “code is speech” argument were low. About that I was wrong, though it turned out not to matter.

A number of the reports noted that after some initial skepticism, Judge Kaplan had been impressed by the defendants’ expert witnesses, particularly those who had testified that code was speech. When the ruling came out, this impression was confirmed. Judge Kaplan agreed that code was a form of speech or expression. But celebration was premature. Having done so, he disagreed with the defendants’ claim that it could not be regulated.

Computer code is expressive. To that extent, it is a matter of First Amendment concern. But computer code is not purely expressive any more than the assassination of a political figure is purely a political statement. Code causes computers to perform desired functions. Its expressive element no more immunizes its functional aspects from regulation than the expressive motives of an assassin immunize the assassin’s action. In an era in which the transmission of computer viruses—which, like DeCSS, are simply computer code and thus to some degree expressive—can disable systems upon which the nation depends and in which other computer code also is capable of inflicting other harm, society must be able to regulate the use and dissemination of code in appropriate circumstances. The Constitution, after all, is a framework for building a just and democratic society. It is not a suicide pact.²

Judge Kaplan is right in saying that there cannot be a bright-line rule immunizing computer code from regulation merely because it has expressive elements. The First Amendment does not protect computer viruses. But the defendants were not arguing that computer code was constitutionally inviolable, only that any law that regulated it had to be subject to First Amendment scrutiny. After all, the government makes the description of how to make a nuclear weapon classified information. That is clearly “speech,” but its regulation is also constitutional. The First Amendment is not, and never was, an absolute guarantee of freedom of speech. Instead, the question is whether the law is within the realm of “the freedom of speech” guarantee, which in turn depends on what kind of a law it is. Where does it fit in the “levels of scrutiny” that courts have constructed to discriminate between types of legislation affecting speech? Is the DMCA a “content-based” regulation, such as a law forbidding labor picketing but allowing other kinds of demonstrations? Content-based regulations are given the highest and most demanding level of scrutiny. Alternatively, is it a “content-neutral” regulation, such as a law that
forbids talking—about any subject—in a library? To Judge Kaplan, the answer was clear, and grounds for sarcasm.

The reason that Congress enacted the anti-trafficking provision of the DMCA had nothing to do with suppressing particular ideas of computer programmers and everything to do with functionality—with preventing people from circumventing technological access control measures—just as laws prohibiting the possession of burglar tools have nothing to do with preventing people from expressing themselves by accumulating what to them may be attractive assortments of implements and everything to do with preventing burglaries.

I agree, though it is worth noting that the burglar tool analogy is a disputed one. Johansen claimed DeCSS was more like a screwdriver—something with both licit and illicit uses.

So the DMCA was content-neutral regulation. That means it still has to pass a fairly daunting legal threshold. It will only be upheld if “it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.” Judge Kaplan felt that the DMCA satisfied that standard. I am not so sure. Yes, the governmental interest in protecting copyright holders’ rights is important. And yes, I must disagree with some of my friends in the civil liberties world and say that the government’s interest is unrelated to the suppression of free expression. But is “the incidental restriction of First Amendment freedoms no greater than is essential to the furtherance of that interest”? In other words, could the DMCA have achieved its goals without imposing as great a limitation on the expression of people like Mr. Johansen and Mr. Corley?

Congress could have passed many laws less restrictive than the DMCA. It could have only penalized the use of programs such as DeCSS for an illicit purpose. If it wished to reach those who create the tools as well as use them, it could have required proof that the creator intended them to be used for illegal purposes. Just as we look at the government’s intention in creating the law, we could make the intent of the software writer critical for the purposes of assessing whether or not his actions are illegal. If I write a novel detailing a clever way to kill someone and you use it to carry out a real murder, the First Amendment does not allow the state to punish me. If I write a manual on how to be a hit man and sell it to you, it may. First Amendment law is generally skeptical of statutes that impose “strict liability” without a requirement of
intent. But Judge Kaplan believed that the DMCA made the motives of Mr. Johansen irrelevant, except insofar as they were relevant to the narrowly tailored exceptions of the DMCA, such as encryption research. In other words, even if Mr. Johansen made DeCSS so that he and his friends could watch DVDs they purchased legally on computers running Linux, they could still be liable for breaking the DMCA.

The DMCA’s breadth goes further than its treatment of intent. The statute could have only made it illegal to provide a program yourself. But Judge Kaplan interpreted it to prohibit even linking to a site where the program is to be found. No requirement of intent. No requirement that you actually supply the infringing program. That is a pretty broad interpretation and one which he admits restricts expression. How could he conclude that restrictions this broad were “no greater than essential”? From his rhetoric, the answer is clear. Judge Kaplan believes the story of the Internet Threat I discussed in Chapter 4. He sees DeCSS as a poison. In fact, he thinks it is worse than a poison because it may spread to infect others. It is a disease, a virus. The DMCA is the stern and harsh quarantine required to control it—a digital public health measure. His reasoning is worth quoting at length.

There was a time when copyright infringement could be dealt with quite adequately by focusing on the infringing act. . . . The copyright holder . . . usually was able to trace the copies up the chain of distribution, find and prosecute the infringer, and shut off the infringement at the source. In principle, the digital world is very different. Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and perfectly copying plaintiffs’ copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. . . . The process potentially is exponential rather than linear. Indeed, the difference is illustrated by comparison of two epidemiological models describing the spread of different kinds of disease. In a common source epidemic, as where members of a population contract a non-contagious disease from a poisoned well, the disease spreads only by exposure to the common source. If one eliminates the source, or closes the contaminated well, the epidemic is stopped. In a propagated outbreak epidemic, on the other hand, the disease spreads from person to person. Hence, finding the initial source of infection accomplishes little, as the disease continues to spread even if the initial source is eliminated.\footnote{11}

This is a very good point, and one that the critics of the DMCA sometimes gloss over too quickly. The structure of digital replication is indeed different from the old centralized model of copying and distribution. Instead of trac-
ing all illicit copies back to a single infringing printing press, we face the fear that the machinery of piracy can be copied just as fast as the copies it allows us to make.

It is here that the defendants lose the battle of the metaphors. Yes, code is speech, it conveys information. But viruses are codes and they convey information too. Judge Kaplan explicitly invokes this comparison several times. Biological viruses are tools for the replication of genetic information. They subvert their hosts’ cellular programming to make copies of themselves, just as a computer virus hijacks an infected computer and causes it to send out more copies of the virus. True, DeCSS requires human intervention to download the program and use it. Yet from Judge Kaplan’s language it is evident that he sees the program not as an act of expression but as a virus spreading like wildfire. Seen this way, the individual “choices” to download or redistribute are simply the program’s method of spreading itself, like the irritation produced by the cold virus that encourages sneezes and coughs, thereby transmitting the illness to others. Just as in an epidemic, the harshest measures are called for. There is no poisoned well here, no pirate with a printing press we can shut down. Anyone is potentially an infringer. Individuals cannot be presumed to be healthy. We cannot give their immune systems, or their motives, the benefit of the doubt. Instead we must see them as potential carriers. The healthy must be quarantined as well as the sick. Facing such a danger, Judge Kaplan agrees that Congress needed to be draconian. We cannot wait for illegal copying. We must strike preemptively at the technology that might enable it. There is no place for inquiries into “intent” here; no way that we can restrict liability to those who actually provide the program. Thus, though “code is speech” and the DMCA does incidentally restrict expression, Judge Kaplan concludes that its restraints are no greater than is necessary.

There are three questions here. The first is whether Congress was right. The second is whether, in the context of the movie industry, we can see evidence of the evil it needed to combat. The third question is very different: whether the DMCA is constitutional. In my opinion, the answer to questions one and two is no, for the reasons outlined in Chapter 4’s analysis of the Internet Threat. Yes, cheaper copying can increase the rate of illicit copying, but it also lowers advertising costs and offers new business models—Netflix, downloads on demand, viral distribution of trailers, and so on. The technology helps as well as hurts. It does not help the movie industry as much as it might help the music industry, which can more easily distribute its products over the Internet. But the Internet also does not pose as much danger to movies as it does to music.
The movie industry’s doomsaying aside, there is no exact movie equivalent of Napster and there is unlikely to be one in the near future.

This is not just because movies are longer and harder to download than songs. It is because most people only watch a film once. Most people do not want a library of two thousand films to play again and again. Music is a repeated experience good in a way that movies simply are not, and that social fact profoundly affects the likelihood of downloading as opposed to rental. The transient song on a radio or an Internet stream is not an adequate substitute for possessing the song permanently—something which costs a lot more. Apart from kids’ movies, which can be used to induce catatonia in one’s progeny time and again, and a few classic favorites, most people do not want to own movies. Watching the film on television or renting it for a night is perfectly satisfactory. Both of these involve little hassle or cost. The content industries are fond of saying “you cannot compete with free.” But this is simply not true. Cheap and easily acquired goods of certified quality compete very well with free goods of uncertain quality whose acquisition involves some difficulty. This is one of the main reasons the movie companies were wrong in the Sony case.

Thus while Judge Kaplan’s discussion of the looming digital Black Death is nicely apocalyptic, it does not seem very accurate. How many of your friends download movies illicitly over the Internet, let alone movies that were ripped from DVDs? Yes, it can be done. But the actual descriptions of the process in the Reimerdes case smack more of bathos than terror.

Although the process is computationally intensive, plaintiffs’ expert decrypted a store-bought copy of Sleepless in Seattle in 20 to 45 minutes. . . . The decryption of a CSS-protected DVD is only the beginning of the tale, as the decrypted file is very large. . . . One solution to this problem, however, is DivX, a compression utility available on the Internet that is promoted as a means of compressing decrypted motion picture files to manageable size. . . . While the compressed sound and graphic files then must be synchronized, a tedious process that took plaintiffs’ expert between 10 and 20 hours, the task is entirely feasible. . . . At trial, defendants repeated, as if it were a mantra, the refrain that plaintiffs, as they stipulated, have no direct evidence of a specific occasion on which any person decrypted a copyrighted motion picture with DeCSS and transmitted it over the Internet. But that is unpersuasive. Plaintiffs’ expert expended very little effort to find someone in an IRC chat room who exchanged a compressed, decrypted copy of The Matrix, one of plaintiffs’ copyrighted motion pictures, for a copy of Sleepless in Seattle. While the simultaneous electronic exchange of the two movies took approximately six hours, the computers required little operator attention during the interim.
So the epidemic threat that hangs over the movie industry consists of the danger that someone will spend fifteen minutes decrypting and ten to twenty hours tediously synchronizing a movie that is then available for a speedy six-hour download?

Admittedly, someone only needs to do the synchronizing once. There are newer tools that make the task easier. And we could improve the download time. But even so, would you bother? Faced with the colossal expense and hassle of renting the same movie at Blockbuster for $3, some consumers might prefer this process, I suppose. But I would not sell my shares in movie studios quite yet. In fact, the real threat to movie studios is the large-scale criminal distribution of illicitly copied DVDs—copied bit for bit from the original. The distributors of those do not need to use programs like DeCSS. A more distant threat comes from legal recordings from television made on TiVo’s and ReplayTVs—where consumers’ actions are legal and CSS is not an issue. So far as we can tell, there is no measurable effect of illicit digital downloads on sales or rentals of DVDs. We could go through the process Judge Kaplan describes, I suppose, just as when the VCR was invented we could have taped movies from television and swapped them with our friends. But as the movie studios discovered after the Sony case, most of us would rather just rent the movie. Because something is possible does not mean it will happen.

So in my view, Congress generally overestimated the threat posed by the digital world and underestimated the benefits. In addition, the movie industry is a weak place to make the case for the necessity of the DMCA. Fine, but that is not the legal issue here. The constitutionality of the DMCA does not turn on whether the DMCA was a good idea. That is not the court’s decision to make. The question is not even whether the particular industry involved is, in reality, facing much of a threat from digital downloading. The law, after all, exists for all digital works, not just the ones at issue here. The question is whether the restriction on speech imposed by the DMCA was “no greater than is essential.” And that is a harder question.

I still disagree with Judge Kaplan. A more narrowly tailored statute could have accomplished the DMCA’s legitimate goals without impinging as greatly on expression. I think that the rhetoric of the Internet Threat blinded Judge Kaplan to some important issues and led him to overestimate the danger and thus the severity of the measures necessary to combat it. Thus, even under the “code is speech” part of the analysis, I think the DMCA fails First Amendment
scrutiny. But if we are confining ourselves to the expression inherent in the software itself, I acknowledge that it is a close call.

Sadly, Judge Kaplan spent much less time on the other First Amendment argument against the DMCA—that it is unconstitutional because it gives copyright holders a new intellectual property entitlement, created by Congress under the Copyright Clause, a legal power to deprive users of a constitutionally required limitation on copyright’s exclusive rights. In my view, he also framed the argument wrongly when he did discuss it. To be fair, these problems can partly be traced to the fact that the defendants spent most of their energy on the argument that code was expression, paying less attention to everything else. As Judge Kaplan explained it, the claim was that the DMCA might have the effect of restricting an alleged fair use right of access to copyrighted material. Predictably enough, he responded that there was no such right of access. Copyright holders could always lock up the book or restrict entrance to the gallery. In any event, while fair use of DVDs might be curtailed, he argued that most movies are also available on videotape. Even if the film were only available on DVD, the prospective fair user could write down the words and quote them, or record the sound from the screen. Finally, Judge Kaplan pointed out that even if the DMCA might allow a significant erosion of fair use to develop over time, such a problem was not present here. Those making First Amendment claims are sometimes allowed by courts to show that, even if the law as it applied to them were constitutional, it would restrict the First Amendment rights of others. Judge Kaplan declined to apply that doctrine here. In effect, he said “come back when there is a problem.”

On appeal, the case was decided by a panel led by Judge Jon Newman. Here the fair use argument received more attention but the result was the same: “Come back when there is a problem.” Significantly, both courts pointed out another concern. The DMCA could effectively make copyright perpetual because even though the copyright term would expire, the legally protected encryption would continue, and tools such as DeCSS, which would have allowed access to the public domain work, would be illegal. This is a major issue because it appears to violate both the First Amendment and the Copyright Clause’s requirement of a limited time. The defendants did not spend adequate time on this argument, however, and the courts again left it for later consideration.

The court of appeals saw the defendants’ argument in just the same way as Judge Kaplan had seen it: a claim that there was a fair use right of actual access to the finest version of every work in every medium, on which the DMCA
put a practical limitation. Such a claim was easy to dismiss. There was no such right of guaranteed practical access. Copyright owners could restrict the practical ability to exercise fair use in many ways without the Constitution being involved. In addition, in a world where copyrighted content is frequently available in both analog and digital form, the actual effects of the DMCA might be trivial and were, in any event, constitutionally acceptable. Judge Newman repeated Judge Kaplan’s point that one could always make fair use of the work in a way the DMCA did not reach, such as by videotaping a picture of the screen.

The fact that the resulting copy will not be as perfect or as manipulable as a digital copy obtained by having direct access to the DVD movie in its digital form, provides no basis for a claim of unconstitutional limitation of fair use. A film critic making fair use of a movie by quoting selected lines of dialogue has no constitutionally valid claim that the review (in print or on television) would be technologically superior if the reviewer had not been prevented from using a movie camera in the theater, nor has an art student a valid constitutional claim to fair use of a painting by photographing it in a museum. Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user’s preferred technique or in the format of the original.

Once the issue is framed this way, the case has been lost. I would argue that there are three baseline errors here: a focus on “affirmative rights of access” as opposed to limits on Congress’s power in handing out exclusive rights over expression without their constitutionally necessary limitations, a focus on practical effects of the provisions rather than on formal constitutional limitations on the copyright system over all classes of works, and a confusion between intellectual property rights and physical property rights that goes to the heart of the Jefferson Warning discussed in Chapter 2. The question is not whether users have a constitutionally protected right of practical access to a preferred version of a work. The question is whether it violates the First Amendment for Congress to give to copyright holders an intellectual property right to exempt their copyrighted works in some formats from fair use and other provisions that are necessary for copyright law in general to be constitutional.

Remember my earlier example. What if Congress amended Section 1201 to say “Any copyright owner can make it illegal to make a fair use of a copyrighted work by putting a red dot on their books, records, and films before selling them. It shall be a crime to circumvent the red dot even if, but for the dot, the use would have been fair”? This statute, I think, is clearly unconstitutional. It would be no answer to say that some owners will not use the red dot,
and even for those that do, there will be older, dotless versions still available. It is irrelevant that I might be able to copy down the crucial lines of the book over your shoulder while you read it and thus claim that I, personally, had not circumvented the dot. The unconstitutionality of the statute does not turn on whether the dots might fall off because of bad adhesive, or whether there are many secondhand bookstores in the area, in which undotted volumes can be found. Even if the red dot rule were only to be applied to hardback books, or graphic novels, or cassette tapes, it would still be unconstitutional. Nor do we have to wait until the entire marketplace is dominated by red-dotted products before considering the issue. It is no answer to say that even before the red dot rule, copyright holders could always have hidden their works, or locked them in safes, or even negotiated individual contracts with the purchasers that have the effect of limiting fair use. That way of framing it just misunderstands the issue on a fundamental level. The claim is not about the happenstance of practical access or the way that a copyright holder can use physical control of an object or existing tangible property rights to undercut fair use.

The point is that Congress violates the First Amendment when, with respect to any work, it gives me an intellectual property right to prohibit copying and distribution of an expressive work sold in the marketplace and an additional legal power to opt out of the limitations contained in Section 107 over that work. The bundle of rights conveyed by the DMCA does exactly that. It is not the DMCA alone that we must analyze. The question is whether Congress can give the exclusive rights contained in Section 106 of the Copyright Act over a particular class of works (say digital works), if it also gives a new right to prohibit citizens from gaining access to those works for the purposes of making a fair use. If Judge Kaplan and Judge Newman are correct, then the DMCA gives an entirely new intellectual property right (technically, a legal power) to the copyright holders to do exactly that. To put it the other way around, the DMCA substracts from the citizen’s bundle of entitlements under federal copyright law, the right (technically, lawyers would call it a privilege) to gain access to a work legally in his possession for the purpose of making a fair use. It is that rule change that is unconstitutional, I would argue, and the way Judge Kaplan and Judge Newman frame that issue makes them miss the point.

Framing is important. The confusions that I have talked about in this book all make an appearance. It starts with the whole controversy being framed by the Internet Threat storyline from Chapter 4. Because Judge Kaplan is convinced that every citizen is now a potential infringer, a potentially infectious virus carrier, he is ill disposed to listen to claims about fair use. Civil liberties
claims do not do very well in epidemics. It is only right for him to defer to Congress’s perception of the problem and the solution, of course. But he buys so deeply into the magnitude of the threat, the extent of the potential piracy pandemic, that it is very hard for him to take seriously the idea that even here there is a legitimate constitutional fair use claim.

The Sony Axiom from Chapter 4 is also ignored, or at least undervalued. As I pointed out there, without a robust set of exceptions and limitations on copyright, the idea that cheaper copying requires greater control will inexorably drive us toward the position that the technologies of cheaper reproduction must be put under the governance of copyright holders. The DMCA continues that logic; its drafters concluded that the right to get access to digital works for purposes of making a fair use must be taken from the bundle of rights possessed by citizens, while the right to enjoin both access and the technologies of access is added to those of copyright holders. Never mind the correctness of such a conclusion as a matter of policy. Are there constitutional limitations on Congress taking such an action? Kaplan and Newman in effect tell us, “not yet.”

More important than the perception of the threat is the understanding of what intellectual property is all about. In Chapter 2, Jefferson warned us that intellectual property rights are not like physical property rights. In analyzing the DMCA, where do we turn for analogies? To physical property, violence, and theft. The cases analyzing the DMCA are full of analogies to trespass, to breaking and entering, to burglars’ tools, and to safecrackers. Private property carries a lot of baggage with it, but we know it well—it is the place we naturally turn for insight. Even I, in order to point out some of the difficulties with those analogies, had to turn to farmers and barbed wire and public rights-of-way along highways. There is nothing wrong with analogies. They help us understand things that are new by comparing them to things we think we understand better. Analogies are only bad when they ignore the key difference between the two things being analyzed. That is what happens here.

Jefferson reminded us that intellectual property rights are clearly artifacts of state creation, monopolies whose internal limitations in scope, duration, and so on are just as important as the rights themselves. Jefferson doubts whether even property rights over land can be understood as natural and absolute—copyrights and patents, which cover subject matter that can be infinitely reproduced without diminishing its substance, clearly cannot. They frequently involve a claim to control purchasers’ behavior with respect to some aspect of an artifact after it has been sold to them in the marketplace, making simpleminded
analogy to “breaking and entering” inappropriate—the extent of the property in question is precisely the issue in dispute. (When Johansen was tried in Norway under the national computer crime law, the court laconically observed that he had bought the DVDs, and one cannot break into one’s own property—effectively turning the analogy on its head.) Jefferson starts from the baseline that monopoly is the exception and freedom is the rule—any limitations on that freedom have to be justified. That is why he always discusses the right and the limitations on the right as an inseparable pair. One cannot discuss them in isolation.

Kaplan and Newman are fine, thoughtful judges. They do not altogether ignore those points. But look how the analysis is set up. At several points in the discussion, there seems to be the assumption that copyright owners have entitlements to total control as of right and that fair use is a mere lucky loophole which, because it can be negated by the happenstance of whether one can get physical access, can hardly have major First Amendment status. They keep pointing out that physical control and tangible property rights frequently allow copyright holders to make fair use impracticable. “And so what?” Jefferson might have responded. This is a classic non sequitur. The question is whether the Congress has the power to add a new right of access-denial to the intellectual property monopoly it is constructing, undermining—as to some works and some fair uses—the balance that the law sets up. The citizen is not pleading for a new right of access, trumping all physical restraint and tangible property rights. The citizen is claiming that Congress has no power to give exclusive rights to restrain copying of digital content while simultaneously taking away the citizen’s existing right to get access to that content for the purposes of fair use—at least in those cases where access is physically possible and violates no other property right, real or intellectual.

The Constitution does not require the United States to break into President Nixon’s desk to get me his tapes, buy me a tape recorder, or give me a right to 18.5 minutes on the broadcast airwaves to play them. But if I can get access to the tapes legally, it does forbid the government from giving President Nixon the power to put a red dot on those tapes and thus claim an intellectual property right to stop me playing them on TV or digitizing them to make the sounds clearer. The restraints imposed by physical happenstance and tangible property rights are different from those imposed by copyright—a congressionally created monopoly over expression. We cannot assume because one is constitutionally acceptable that the others are too. Jefferson understood that, and his analysis can help us even in a constitutional conflict.
over a technology he could hardly have dreamt of. (Though perhaps with Jefferson, this is a bad bet.)

The same point comes up in a different way when the court disconnects the fair use discussion from the exclusive rights discussion. The question is not “Do I have a constitutionally protected right of physical access to a preferred version of a movie, so as to make my task easy?” That gets the court caught up in questions of when a majority of movies will only be available on DVD, or how poor a substitute the analog version would be, or how many fair uses will require actually cutting a digital fence. But all of these inquiries miss the point. The question is “Can Congress hand out the exclusive rights of copyright over digital works if it does not accompany those rights with the suite of limitations that the court has repeatedly said ‘saves’ copyright from violating the First Amendment?” The proportion of digital works to the total number of works produced in other formats is irrelevant. As to these works, the rule is unconstitutional. But what about the number or proportion of types of fair uses affected? That is more relevant but still not dispositive in the way Kaplan and Newman imagined. True, not every trivial statutory modification of fair use makes copyright unconstitutional. But this is not a trivial modification: over an entire class of works, copyright owners are given a legal power to deprive users of their privilege to gain otherwise lawful access for the purposes of fair use. If you give the digital filmmaker the exclusive rights of copyright but forbid the film professor from going through the otherwise lawful process of parodying or quoting, that rule is unconstitutional, no matter how many other fair uses are unaffected. If the copyright law were amended to forbid journalists playing, on a Friday, excerpts of legally acquired red-dotted tapes made by presidents whose last name begins with N, it would still be unconstitutional.

The legal implementation of this conclusion would be simple. It would be unconstitutional to punish an individual for gaining access in order to make a fair use. However, if they cut down the digital fence to make illicit copies, both the cutting and the copying would be illegal. But what about the prohibition of trafficking in digital wire cutters, technologies such as DeCSS? There the constitutional question is harder. I would argue that the First Amendment requires an interpretation of the antitrafficking provisions that comes closer to the ruling in the Sony case. If Mr. Johansen did indeed make DeCSS to play DVDs on his Linux computer, and if that were indeed a substantial noninfringing use, then it cannot be illegal for him to develop the technology. But I accept that this is a harder line to draw constitutionally. About my first conclusion, though, I think the argument is both strong and clear.
Ironically, there is some support for my claim and it comes from an even higher, if not uniformly more thoughtful, set of judges than Newman and Kaplan. In the depressing case of *Eldred v. Ashcroft*, the Supreme Court upheld retrospective copyright term extensions against a variety of constitutional challenges. (Full disclosure: I assisted in the preparation of an amicus curiae brief in the case.) One of those challenges was based on the First Amendment. The fairly reasonable claim was that Congress could not retroactively lock up an entire twenty-year swathe of culture that had already been produced. Such a law would be all restraint of expression, performance, republication, adaptation, and so on, *with no incentive benefits*. The Court was unconvinced. But it did say:

> To the extent such assertions raise First Amendment concerns, copyright's built-in free speech safeguards are generally adequate to address them. We recognize that the D.C. Circuit spoke too broadly when it declared copyrights "categorically immune from challenges under the First Amendment." . . . But when, as in this case, *Congress has not altered the traditional contours of copyright protection*, further First Amendment scrutiny is unnecessary.\(^\text{14}\)

The DMCA, of course, does exactly this. As to digital works it alters the “traditional contours of copyright protection” in a way that affects “copyright’s built-in free speech safeguards.” That is what the Farmers’ Tale was all about. Perhaps one day, in a case not involving a Norwegian teenager, a hacker magazine run by a long-haired editor with an Orwellian nom de plume, and an obscure technology that is accused of posing apocalyptic threats to the American film industry, that point will come out more clearly.

But the issue of speech regulation is only half of the story. Intellectual property rights over digital technologies affect not only speech, but the framework of competition and markets as well, as the next example makes clear.

**The Apple of Forbidden Knowledge: The DMCA and Competition**

You could tell it was a bizarre feud by the statement Apple issued, one strangely at odds with the Californian Zen-chic the company normally projects. “We are stunned that RealNetworks has adopted the tactics and ethics of a hacker to break into the iPod, and we are investigating the implications of their actions under the DMCA and other laws.”\(^\text{15}\)

What vile thing had RealNetworks done? They had developed a program called Harmony that would allow iPod owners to buy songs from Real’s Music
Store and play them on their own iPods. That’s it. So why all the outrage? It turns out that like the story of DeCSS, this little controversy has a lot to teach us about the landscape of intellectual property disputes, about the mental topography of the high-tech economy. But where the DeCSS case was a war of metaphors around the boundaries of freedom of expression, the iPod story is about ways in which intellectual property marks the limits of competition.

Apple iPods can be used to store all kinds of material, from word processing documents to MP3 files. If you want to use these popular digital music players to download copy-protected music, though, you have only one source: Apple’s iTunes service, which offers songs at 99 cents a pop in the United States, 79 pence in the United Kingdom. If you try to download copy-protected material from any other service, the iPod will refuse to play it. Or at least, that had been the case until Real managed to make their Harmony service compatible.

Real’s actions meant that consumers had two sources of copy-protected music for their iPods. Presumably all the virtues of competition, including improved variety and lowered prices, would follow. The iPod owners would be happy. But Apple was not. The first lesson of the story is how strangely people use the metaphors of tangible property in new-economy disputes. How exactly had Real “broken into” the iPod? It had not broken into my iPod, which is after all my iPod. If I want to use Real’s service to download music to my own device, where’s the breaking and entering?

What Real had done was make the iPod “interoperable” with another format. If Boyle’s word processing program can convert Microsoft Word files into Boyle’s format, allowing Word users to switch programs, am I “breaking into Word”? Well, Microsoft might think so, but most of us do not. So leaving aside the legal claim for a moment, where is the ethical foul?

Apple was saying (and apparently believed) that Real had broken into something different from my iPod or your iPod. They had broken into the idea of an iPod. (I imagine a small, platonic white rectangle, presumably imbued with the spirit of Steve Jobs.) Their true sin was trying to understand the iPod so that they could make it do things that Apple did not want it to do. As an ethical matter, does figuring out how things work, in order to compete with the original manufacturer, count as breaking and entering? In the strange netherworld between hardware and software, device and product, the answer is often a morally heartfelt “yes!” I would stress “morally heartfelt.” It is true manufacturers want to make lots of money and would rather not have competitors. Bob Young of Red Hat claims “every business person wakes up in the morning and says ‘how can I become a monopolist?’ ” Beyond that, though,
innovators actually come to believe that they have the moral right to control
the uses of their goods after they are sold. This isn’t your iPod, it’s Apple’s iPod.

Yet even if they believe this, we don’t have to agree. In the material world,
when a razor manufacturer claims that a generic razor blade maker is “stealing
my customers” by making compatible blades, we simply laugh. The “hacking”
there consists of looking at the razor and manufacturing a blade that will fit.
To say this is somehow immoral seems laughable. Is the conclusion changed
when the information about compatibility is inscribed in binary code and
silicon circuits, rather than the molded plastic of a razor cartridge? What if
ensuring the “fit” between the two products is not a matter of making sure the
new blades snugly connect to the razor but of making sure the software
embedded in my generic product sends the right code to the original product
in order to be recognized? Our moral intuitions are a little less confident here.
All kinds of bad policy can flourish in that area of moral uncertainty.

This leads us to the law. Surely Apple’s suggestion that the DMCA might
prohibit what Real had done is as baseless as their moral argument? In the
United States, the answer is “probably,” at least if the courts continue in the
direction they are currently taking, but it is a closer call than you would think.
Internationally, the answer is even less certain. That is where the iPod war pro-
vides its second new-economy lesson. Think for a moment about the way that
the law shapes the business choices in this dispute.

In a competitive market, Apple would choose whether to make the iPod an
open platform, able to work with everyone’s music service, or to try to keep
it closed, hoping to extract more money by using consumers’ loyalty to the
hardware to drive them to the tied music service. If they attempted to keep it
closed, competitors would try to make compatible products, acting like the
manufacturers of generic razor blades or printer cartridges.

The war would be fought out on the hardware (and software) level, with the
manufacturer of the platform constantly seeking to make the competing prod-
ucts incompatible, to bad-mouth their quality, and to use fear, uncertainty, and
doubt to stop consumers from switching. (Apple’s actual words were: “When
we update our iPod software from time to time, it is highly likely that Real’s
Harmony technology will cease to work with current and future iPods.”) Mean-
while the competitors would race to untangle the knots as fast as the platform
manufacturer could tie them. If the consumers got irritated enough they could
give up their sunk costs and switch to another product altogether.

All of this seems fine, even if it represents the kind of socially wasteful arms
race that led critics of capitalism to prophesy its inevitable doom. Competition

is good and competition will often require interoperability. But what do we mean by competition? Is it competition if I assassinate your employees or poison the food in your restaurant? If I trespass on your land in order to sell a competing product? If I break into your safe to steal your trade secrets, use my monopoly position in the market to impose resale price agreements, or violate your patent? It is the law that draws the line between competition and theft, between virtuous competitive imitation and illicit “piracy.”

Sometimes we need to give innovators property rights that allow them to prevent second-comers from free riding on their efforts. We have to do so because it is necessary to encourage future innovation. On the other hand, sometimes we not only allow the second-comer to free ride, we positively encourage it, believing that this is an integral part of competition and that there are adequate incentives to encourage innovation without the state stepping in. Intellectual property policy, indeed a large part of the policy behind all property rights, is about drawing the line between the two situations. Too far in one direction and innovation suffers because potential investors realize good ideas will immediately be copied. Too far in the other direction and monopolies hurt both competition and future innovation.

Imagine you are the first person to invest in getting the public to eat burritos for breakfast, or to place a petrol station at a certain crossroads, or to clip papers together with a folded bit of wire. In each case we give you some property rights. The fast-food vendor may own a trademarked phrase or jingle that the public learns to associate with his product. Since the patent office issued a patent for the sealed and crimped “peanut butter and jelly” sandwich I described at the beginning of the book, even a patent is not out of the question if your disgusting concoction is sufficiently novel and nonobvious. But we should not allow you to have a patent over all burritos, or burritos for breakfast, still less over the idea of fast food. As for the paper clip maker, there might be a trademark over the particular paper clip, but the idea of folding wire to secure paper stays in the public domain. The owner of the petrol station gets physical ownership of the land, but cannot stop a second-comer from setting up shop across the road, even if the first-comer’s labor, capital, and effort proved that the location is a good one. We positively encourage follow-on imitation in those cases.

Now how about the case in point? What does Apple get in the way of property rights? Think back to my description of the intellectual property system in Chapter 1. They can get patents over those aspects of the iPod—both hardware and software—that are sufficiently innovative. Patents are what we use...
to protect inventions. They also get a copyright over the various pieces of software involved. That protects them only against someone who copies their code, not someone who writes new software to do the same thing. Copyrights are what we use to protect original expression. They get rights under trademark law over the name and perhaps parts of the design of the product—maybe the distinctive look of the iPod—though that is a bit more complex. All of these rights, plus being the first to break into the market in a big way, the brilliance of the design, and the tight integration between the hardware and the service, produce a formidable competitive advantage. The iPod is a very good product.

Now if a competitor infringes any of Apple’s rights, for example by making a literal copy of the code, using their trademark in a way the law does not allow, or infringing on one of their patents, then Apple can shut them down and extract hefty damages. Quite right, too. But should they be able to prevent someone from making an interoperable product, provided they do not violate any of these existing rights in the process? Laws like the DMCA make that question more complicated.

Nowadays, there is software in many, many more products than you would imagine. Your watch, your phone, your printer, your thermostat, your garage door opener, your refrigerator, your microwave, your television—the odds are that if you bought them in the last ten years, they have some software component. In the 1970s the courts and Congress had concluded that software could be copyrighted as original expression, like a song or a novel, as well as being patented when it was novel, nonobvious, and useful. Frequently, different aspects of the same program will be covered by copyright and by patent. But software is a machine made of words, the machine of the digital age. That fact already causes some problems for our competition policy. Will the exceptions and limitations designed to deal with a copyright over a novel work adequately when they are applied to Microsoft Windows? That issue was already unclear. With the DMCA, we have added another crucial problem. Where there is copyrighted software there can be digital fences around it. If the copyright owner can forbid people to cut these fences to gain access to the software, then it can effectively enlarge its monopoly, capture tied services, and prohibit generic competition.

It was just this line of thought that led some other companies to do more than merely make threatening noises about the DMCA. Lexmark makes printers. But it also makes lots of money off the replacement ink or toner cartridges for those printers. In some cases, in fact, that is where printer companies make
the majority of their profits. As a result, they are not exactly keen on generic replacements. Chamberlain makes garage door opener systems. But they also sell replacements for the controllers—the little devices that you use to trigger the door. Lawyers from both of those firms looked at the DMCA and saw a chance to do something most companies would love to do; to make generic competition illegal. Lexmark designed their printer program so that it would not accept a toner cartridge unless it received the correct “checksum” or validation number. So far, this looks no different from the razor manufacturer trying to make it difficult to manufacture a compatible replacement blade. Generic competitors now had to embed chips in their printer cartridges which would produce the correct code, otherwise they would not work in Lexmark printers.

Static Control Components is a North Carolina company that manufactures chips whose main function is to send the correct code to the printer program. With this chip implanted in them, generic cartridges would work in Lexmark printers. Lexmark’s response could have been to change their program, rendering the chip obsolete, just as Apple could change the iTunes software to lock out Real Music’s Rhapsody. Doing so would have been quite within their rights. Indeed it is a standard part of the interoperability wars. Instead, Lexmark sued Static Controls, claiming, among other things, a violation of the DMCA. Like Apple in the press release I quoted earlier, Lexmark clearly saw this as a kind of digital breaking and entering. This was their printer, their printer program, their market for replacement cartridges. Static was just helping a bunch of cheats camouflage their generic cartridges as authentic Lexmark cartridges. Translated into the legal language of the DMCA the claim is a little different, but still recognizable. Static was “trafficking” in a device that allowed the “circumvention of a technical protection measure” used to prevent “access to a copyrighted work”—namely the computer program inside the printer. That is behavior that the DMCA forbids.

The garage door company, Chamberlain—who also claimed to be concerned about the security of their garage doors—made a similar argument. In order to get the garage door to open, the generic replacement opener had to provide the right code to the program in the actual motor system. That program is copyrighted. The code controls “access” to it. Suddenly, the manufacturers of generic printer cartridges and garage door openers start to look rather like Jon Johansen.

Surely the courts did not accept this argument? Bizarrely enough, some of them did—at least at first. But perhaps it was not so bizarre. The DMCA
was indeed a radical new law. It did shift the boundaries of power between intellectual property owners and others. And intellectual property rights are always about restraining competition, defining what is legitimate and what is not—that is what they do. There was a respectable argument that these devices did in fact violate the DMCA. In fact, it was respectable enough to convince a federal judge. The district court judge in the *Lexmark* case concluded that *Lexmark* was likely to win on both the DMCA claim and on a more traditional copyright claim and issued an injunction against Static Control. In *Skylink*, the case involving garage door openers, by contrast, the district court held that the universal garage door opener did not violate the DMCA. Both cases were appealed and both appeals courts sided with the generic manufacturers, saying that the DMCA did not prohibit this kind of access—merely making a computer program work the way it was supposed to.

The U.S. Court of Appeals for the Federal Circuit (CAFC) heard the *Skylink* appeal. In a remarkably far-reaching decision, the court effectively took many of the positions that Mr. Corley’s lawyers had argued for in the DeCSS case, but they did so not to protect speech, but to protect competition. In fact, they implied that taking Chamberlain’s side in the case would silently overrule the antitrust statutes. They also interpreted the new right created by the DMCA so as to add an implicit limitation. In their construction, merely gaining access is not illegal; only gaining access for the purpose of violating the copyright holders’ rights violates the statute. The *Reimerdes* court had been willing to accept that the new access right allows a copyright holder to prohibit “fair uses as well as foul.” When Chamberlain made the same argument as to their garage door opener program, the CAFC was incredulous.

Such an entitlement [as the one Chamberlain claims] would go far beyond the idea that the DMCA allows copyright owner to prohibit “fair uses ... as well as foul.” *Reimerdes*, 111 F. Supp. 2d at 304. Chamberlain’s proposed construction would allow copyright owners to prohibit exclusively fair uses even in the absence of any feared foul use. It would, therefore, allow any copyright owner, through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work—or even selected copies of that copyrighted work.17

There are multiple ironies here. The CAFC rarely meets an intellectual property right it does not like. It has presided over a twenty-year expansion of
American patent law that many scholars find indefensible. But when (for dubious jurisdictional reasons) it sorties beyond its traditional ambit of patent law, it is stunned by the potential expansiveness of the DMCA. Then there is the comparison with the Reimerdes case. How interesting that the First Amendment and concerns about free expression have comparatively little bite when applied to the DMCA, but antitrust and concerns about competition require that we curtail it. After all, the heart of Mr. Johansen’s argument was that he had to write the DeCSS program in order to play his own DVDs on his own computer—to get access to his own DVDs, just as the purchaser of a replacement garage door control is getting access to the program that operates his own garage door. Indeed, Mr. Johansen’s criticism of CSS was that it allowed the movie companies, “through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work.” Mr. Corley echoed those claims.

Of course, the situations are not identical. The key limitation in Skylink is that the court saw no threat of “foul use.” The Reimerdes court could see little else. On the other hand, the rulings are not easily reconciled. The Skylink court cannot imagine that Congress would want to give the copyright holder a new “property” right to prevent access unconnected to any underlying copyright violation.

As we have seen, Congress chose to create new causes of action for circumvention and for trafficking in circumvention devices. Congress did not choose to create new property rights. . . . Were we to interpret Congress’s words in a way that eliminated all balance and granted copyright owners carte blanche authority to preclude all use, Congressional intent would remain unrealized.

Yet, arguably, that is exactly what the Reimerdes decision does, precisely because it focuses on enabling access alone, not access for the purpose of violating one of the rights of the copyright holder. The Reimerdes court saw a violation of the law just in cutting the wire or making a wire cutter. The Skylink court focused on whether the person cutting the wire was going to trespass once the cutting was done. In effect, the two courts disagree on which of the options offered to the legislature in the Farmers’ Tale was actually enacted by Congress. Which court is correct? The Skylink decision strikes me as sensible. It also makes the statute constitutionally much more defensible—something that the Skylink court does not consider. But in the process, it has to rewrite the DMCA substantially. One should not presume that it will be this interpretation that will triumph.
SUMMING UP: EXAGGERATIONS, HALF-TRUTHS, AND BIPOLAR DISORDERS IN TECHNOLOGY POLICY

Let me return to the question with which I began the chapter. For many critics of contemporary intellectual property law, the DMCA is the very embodiment of all that is wrong. (I still cherish a friend’s account of British protesters outside the American Embassy in London singing “D-M-C-A” to the tune of the Village People’s “YMCA” and holding up signs calling for the law’s repeal—to the great confusion of the diplomatic personnel.) The critics conjure up a digital apocalypse—a world of perfect control achieved through legally backed digital fences, in which both speech and competition suffer, and where citizens lose privacy, the privilege of fair use, and the right to criticize popular culture rather than simply consume it. In their view, the legal disaster is only exacerbated by bumbling judges who do not understand the technology and who are easily fooled by the doom-laden rhetoric of the content companies. The DMCA’s supporters, on the other hand, think criticisms of the DMCA are overblown, that the dark tales of digital control are either paranoid delusions or tendentious exaggerations, and that far from being excessive, the DMCA’s provisions are not sufficient to control an epidemic of illicit copying. More draconian intervention is needed. As for fair use, as I pointed out before, many of the DMCA’s supporters do not think fair use is that important economically or culturally speaking. At best it is a “loophole” that copyright owners should have the right to close; certainly not an affirmative right of the public or a reserved limitation on the original property grant from the state.

Who is right? Obviously, I disagree profoundly with the DMCA’s supporters. I wrote this book partly to explain—using Jefferson and Macaulay and the *Sony* case—what was wrong with their logic. It would be both convenient and predictable for me to claim that the DMCA is the intellectual property incarnation of the Antichrist. But it would not be true. In fact, I would not even put the DMCA in the top three of bad intellectual property initiatives worldwide. And many of the fears conjured up about it are indeed overblown.

Of course, the critics have a point. The DMCA is a very badly drafted law. As I have tried to show here, its key provisions were probably unnecessary and are, in my view, unconstitutional. If coupled with a number of other legal “innovations” favored by the content industry, the DMCA could play a very destructive role. In general, in fact, the Farmers’ Tale is fairly accurate in de-
scribing both the origins of and the threats posed by the DMCA. Yet the single largest of those threats—the idea that the DMCA could be used to fence off large portions of the public domain and to make the fair use provisions of the Copyright Act essentially irrelevant—is still largely a threat rather than a reality. In some cases, fair use rights are curtailed. But for most citizens and for the majority of media, the DMCA has had relatively little effect. Digital rights management (DRM) certainly exists; indeed it is all around us. You can see that every time you try to play a DVD bought in another part of the world, open an Adobe eBook, or copy a song you have downloaded from iTunes. But so far, the world of legally backed digital rights management has not brought about the worst of the dystopian consequences that some people, including me, feared might result.

In many cases, citizens simply reject digital rights management. They will not buy products that use it. Attempts to introduce it into music CDs, for example, have been a resounding failure. In other cases, DRM has not been used in ways that the critics feared. There are genuine scandals, of course—cryptography research has been chilled, the DMCA has been turned to anticompetitive ends, and so on. It is also troubling to see federal judges issuing injunctions not only against banned material but also against those who link to the banned material. Somehow the blithe reassurance that this is consistent with the First Amendment fails to comfort one. But many of the evils prophesied for the DMCA remain as just that: prophecies.

There are also entries on the positive side of the ledger. The “safe-harbors” that the DMCA gave Internet service providers and search services have been a vital and positive force in the development of the Internet. It may even be true that in some cases, such as iTunes, the DMCA did what its backers claimed it would—encourage new provision of digital content by reassuring the record companies that they could put their music online surrounded by legally backed digital rights management. (Notably, however, the trend is now going the other way. Companies are coming to realize that many consumers prefer, and will pay more for, unprotected MP3 files.)

Of course, depending on your view of the music industry, that might seem like a mixed blessing. One might also wonder if the same consumer benefits might have been produced with a much less restrictive law. But with the exception of a few important areas—such as cryptography research, where its effects are reported to be severe—I would have to say that the criticisms focus too much on the DMCA, to the exclusion of the rest of the intellectual property landscape. Yes, the DMCA offers enormous potential for abuse, particularly
in conjunction with some other developments in intellectual property that I will discuss later, but much of the abuse has not yet happened. Yet even if it never did happen, the DMCA has important lessons to teach us.

In this section I have tried to show how legal rules—particularly intellectual property rules—define the boundaries of legitimate competition. We used to assume that this was principally the function of patent and trademark law, less so of copyright. Of course, copyright would affect competition in publishing and in the TV and movie industries, but it hardly seemed central to competition policy in general. But once courts and legislatures accepted that software is copyrightable, that assessment changed. The levers and cogs of the machines of the modern economy are forged out of ones and zeros instead of steel and brass. In that situation, copyright is central to the competition policy of a high-tech economy.

As the Apple case shows, our moral intuitions about competition are going to be cloudier in the world of digital content and cyberspace. The same is true of the law. Even in the material world it can be hard to draw the line between the legitimate and ruthless pursuit of commercial advantage and various forms of unfair competition, antitrust violations, and so on. But in the immaterial world, the boundaries are even harder to draw. Is this the digital equivalent of trespass or legitimate passage on a public road that runs through your property? As I pointed out earlier, the constant analogies to physical property are likely to conceal as much as they reveal. Is this virtuous competitive imitation or illicit copying? We have strong, and by no means coherent, moral and legal intuitions about the answers to such questions. And our legal structure often gives us the raw material to make a very good case for both sides of the argument.

Into this already troubled situation, with a set of rules designed for original expression in novels and poems being applied to machines made of computer code, we add the DMCA and its new rights of uncertain extent. Copyright had a well-developed set of exceptions to deal with anticompetitive behavior. Where the existing exceptions did not function, courts tended to turn to fair use as the universal method for patching the system up—the duct tape of the copyright system. Without an evolving idea of fair use, copyright would overshoot its bounds as it was applied to new technologies and new economic conditions. Indeed that was the point of the Sony Axiom. The DMCA threw this system into disarray, into a war of competing metaphors.

The Skylink court sees monopolists being handed carte blanche to abolish the restraints on their monopolies. Competition policy demands that we
construe the DMCA narrowly. The Reimerdes court sees a virus masquerading as speech, a digital pandemic that must be stopped at all costs by a draconian program of electronic public health. Each proceeds to construe the statute around the reality they have created. It is by no means certain which metaphor will win the day, still less which resolution will triumph in other countries that have passed versions of the DMCA. International attitudes toward speech, competition, and the necessary exceptions in a copyright system vary widely. Yet backed by the story of the Internet Threat, the content companies are already saying that we need to go further both nationally and internationally—introducing more technology mandates, requiring computers to have hardware that will only play approved copyrighted versions, allowing content companies to hack into private computers in search of material they think is theirs, and so on. Remember the suggestion from the beginning of the chapter, that all cars be assumed to be getaway vehicles for the felonious filchers of vegetables, and thus that they should be fitted with radio beacons, have the size of their cargo space reduced, and so on? The Farmers’ Tale continues to evolve.