Policy Analysis

No. 564 March 21, 2006

Circumventing Competition

The Perverse Consequences of the Digital Millennium Copyright Act

by Timothy B. Lee

Executive Summary

The courts have a proven track record of fashioning balanced remedies for the copyright challenges created by new technologies. But when Congress passed the Digital Millennium Copyright Act in 1998, it cut the courts out of this role and instead banned any devices that "circumvent" digital rights management (DRM) technologies, which control access to copyrighted content.

The result has been a legal regime that reduces options and competition in how consumers enjoy media and entertainment. Today, the copyright industry is exerting increasing control over playback devices, cable media offerings, and even Internet streaming. Some firms have used the DMCA to thwart competition by preventing research and reverse engineering. Others have brought the weight of criminal sanctions to bear against critics, competitors, and researchers.

The DMCA is anti-competitive. It gives copyright holders—and the technology companies that distribute their content—the legal power to create closed technology platforms and exclude competitors from interoperating with them. Worst of all, DRM technologies are clumsy and ineffective; they inconvenience legitimate users but do little to stop pirates.

Fortunately, repeal of the DMCA would not lead to intellectual property anarchy. Prior to the DMCA's enactment, the courts had already been developing a body of law that strikes a sensible balance between innovation and the protection of intellectual property. That body of law protected competition, consumer choice, and the important principle of fair use without sacrificing the rights of copyright holders. And because it focused on the actions of people rather than on the design of technologies, it gave the courts the flexibility they needed to adapt to rapid technological change.

Timothy B. Lee is a policy analyst at the Show-Me Institute in St. Louis. He holds a degree in computer science from the University of Minnesota and is the science and technology editor of the online magazine Brainwash *and a contributor to the Technology Liberation Front website.*

CATO INSTITUTE

The DMCA's most profound effects will be on the evolution of digital media technologies.

Introduction

As Robert Frost wrote, good fences make good neighbors. Fences demarcate property lines, enhance privacy, and prevent unauthorized entry. No one would dispute that fences are vital to protecting private property rights.

Yet Congress would be rightly ridiculed if it made it a crime to hop over a fence. Sometimes, hopping a fence is unobjectionable—when you lose a baseball on your neighbor's property, see your stolen bicycle in someone's yard, or know that a fenced lot has been abandoned, for example. More important, such a law would be completely unnecessary, because the common law of trespass already protects property owners against intrusions on their rights. Because it was developed over centuries by judges considering real-world controversies, the law of trespass is flexible, sensible, and predictable, ensuring that individuals can enjoy their property without unduly impeding the people who might have legitimate reasons to cross their property lines.

Digital rights management (DRM) technologies are the fences of the intellectual property world. They control access to digital media to discourage copyright infringement. For example, when a customer purchases a song over the Internet using Apple's iTunes Music Store, Apple's DRM system enforces rules about how the song may be copied. The system permits the customer to copy the song to his iPod, share it with others on his local network, or burn a single copy to a CD, but it does not permit him to upload it to a peer-to-peer file-sharing network, transfer it to a Sony Walkman, or burn a dozen copies to CDs.

In 1998 Congress gave DRM schemes explicit statutory protections when it passed the Digital Millennium Copyright Act. The DMCA not only made it a crime to "circumvent" DRM technologies—to hop intellectual property's fences—but it also prohibited creating or distributing "circumvention devices." It is illegal under federal law to build digital stepladders.

This section of the DMCA was every bit as unnecessary as a federal ban on fence jumping would be. The courts had already successfully addressed several high-tech challenges to copyright law. A body of law analogous to trespass was providing robust, sensible, and flexible protection for intellectual property rights.

In passing the DMCA, Congress short-circuited that evolutionary process. It threw out the accumulated wisdom of legal precedent and replaced it with a rigid and sweeping anti-circumvention rule.

The new legislation's most profound effects will be on the evolution of digital media technologies. We have grown accustomed to, and benefit from, a high-tech world that is freewheeling, open-ended, and fiercely competitive. Silicon Valley is a place where upstarts like Apple, Netscape, and Google have gone from two-man operations to billion-dollar trendsetters seemingly overnight. The DMCA threatens to undermine that competitive spirit by giving industry incumbents a powerful legal weapon against new entrants.

In the name of fighting piracy, the DMCA gives copyright holders—and the companies that distribute their material—legal tools that can control who makes products compatible with their technology platforms and able to access their content. Examples can be seen in each of the next-generation platforms for video entertainment, including prerecorded home video, cable and interactive television, and even streaming Internet media. Copyright holders have used the DMCA as a contract enforcement tool, promoted criminal actions against programmers who expose flaws in DRM software, and worked to suppress academic research that affects copyright protection.

Not only is that bad for innovation and entrepreneurship, it is bad for consumers as well. Ordinarily, new technologies allow us to consume media in new ways. The VCR introduced the idea of taping shows for later viewing. The invention of MP3 players like the iPod allowed consumers to put their entire music libraries in their pockets. Software emulators allowed consumers to play games designed for popular consoles like the PlayStation on their computers. In each of those cases, industry incumbents sought to use the legal process to

block the technologies, arguing that they violated copyright law. And in each case, the courts rebuffed the industry's efforts, holding that copyright law is designed to promote, not impede, technological progress.

The DMCA puts its thumb on the scales of justice on the side of copyright holders. Digital rights management technologies give copyright holders complete control over every aspect of how their products are used. And the DMCA gives DRM technologies the force of law. As a result, when the next VCR or iPod is invented, the content industry may use its powers under the DMCA to refuse to allow its content to be used on the new device.

If new inventions are prevented from even entering the marketplace, there will never be an opportunity for a public debate about their benefits. Most consumers will not even know what they are missing.

High-Tech Challenges for Copyright Law

Copyright law gives authors, artists, musicians, and other creators broad, exclusive rights to commercial exploitation of their creations. With certain limitations, the copyright holder is granted the exclusive right to make and distribute copies of its works. Thus, copyright is designed to promote cultural progress by encouraging the production of new creative works.

Congress has been mindful of the danger that copyright could itself become an obstacle to progress by unduly inhibiting the free flow of ideas. To forestall that threat, Congress placed careful limits on the scope of creators' rights under the law. For example, facts cannot be copyrighted, although a particular description of facts can be. Copyrights are granted for limited times, after which the material falls into the public domain. The first sale doctrine gives consumers the right to resell legitimately purchased copies of copyrighted material to others. And the doctrine of fair use holds that certain kinds of innocuous copying—such as including a short excerpt in a book review or recording a TV program for later viewing—are not violations of copyright.

Technological progress has thrown questions about the limits of copyright into stark relief. Digital technologies give ordinary consumers far greater abilities to make unauthorized copies than ever before. Sorting out which of those copies are infringing under copyright law has not been easy. Fortunately, the courts have consistently risen to the challenge, developing nuanced legal doctrines that protect the rights of intellectual property holders without unduly burdening high-tech innovation.[1] Important recent intellectual property decisions demonstrate that the courts have struck a sensible balance that protects both innovation and intellectual property.

Copyrighted Software and "Clean Room" Design

One frequent subject of copyright litigation is the practice of reverse engineering. Reverse engineering is disassembling a hardware or software product from another company to find out how it works with the intention of duplicating some or all of its functions in another product. For decades high-tech companies have sought to use intellectual property law to create proprietary technology platforms over which they would have complete control. Almost from its inception in the 1970s, the computer industry has seen bitter legal feuds in which entrenched incumbents have sought to use copyright law to prevent competitors from building products compatible with their systems.

An early example of that fight was in the market for "IBM-compatible" computers in the 1980s. IBM created that market in 1981 with the release of the IBM PC, its response to the popular Apple II personal computer. Thanks to the strength of the IBM brand, it quickly became a leading business computer.

Every IBM PC contained software known as the Basic Input Output System (BIOS), and no IBM-compatible PC could function without a BIOS of its own. When other companies began making unauthorized "clones" of the computers, most of them simply put a copy of

The courts have developed nuanced legal doctrines that protect the rights of intellectual property holders without unduly burdening high-tech innovation.

the IBM BIOS in their products. Since the BIOS was copyrighted software, IBM easily shut them down in court, as courts held that software may not be copied without permission, even for the purpose of ensuring compatibility with a competitor's product.[2] In other words, compatibility does not justify piracy.

However, in 1984 clones began appearing with a BIOS developed by Phoenix Technologies that was not a copy of IBM's BIOS. Instead, Phoenix had developed its BIOS using a so-called clean room development process, using two separate teams of engineers. The first team studies the product to be emulated (in this case IBM's BIOS) and learns every detail of how it works. It then writes the complete specifications of the product, describing every feature in detail but being careful not to include any of the original product's copyrighted software. A second team of engineers, none of whom has ever seen the original product, then develops a new product based only on the specifications provided by the first team. No other communication between the two teams is permitted. If each team does its job well enough, the result is a product that works exactly like the original product without including any copyrighted material.

Phoenix succeeded in creating a BIOS that performed exactly like IBM's version, and its development process was so airtight that IBM did not even bother filing a copyright infringement lawsuit.[3] The first crop of "IBM clones," whose successors still dominate the market today, were created with Phoenix's BIOS. Their success helped to legitimize the clean room process.

That legitimacy was confirmed by the 1992 case of *Sega v. Accolade*.[4] Sega Enterprises attempted to use copyright law to prevent competitor Accolade from producing unauthorized games for Sega's popular Genesis video game console. Accolade had used the clean room technique to reverse engineer the operating software of the Genesis console and produce Genesis-compatible games. In its decision, the U.S. Court of Appeals for the Ninth Circuit not only confirmed that such development does not violate copyright law, but it went further: Even though Accolade's reverse-engineering process required some unauthorized copying of Sega's copyrighted software, the Ninth Circuit held that this was a fair use because there was no other way for Accolade to determine the console's functional requirements, which are facts that cannot be protected by copyright.

The legality of clean room development and reverse engineering was affirmed again in the 2000 case of *Sony v. Connectix*.[5] In that case, Connectix had reverse engineered the Sony PlayStation in order to make a PlayStation emulator, which allowed consumers to play PlayStation games on their computers. Following the *Sega* precedent, the Ninth Circuit Court of Appeals ruled that Connectix had not violated Sony's copyrights in developing the game.

The ability to build interoperable products without the permission or cooperation of entrenched incumbents is vital to high-tech innovation. Recognizing that fact, the courts have carefully distinguished between the right of software developers to profit from their creative efforts and the right of others to create compatible and interoperable products. This is one of several difficult technology-based challenges for copyright that the courts have addressed well.

The ability to build interoperable products without the permission or cooperation of entrenched incumbents is vital to high-tech innovation.

Time Shifting and Space Shifting

The balance between protecting the rights of copyright holders and creating a legal environment conducive to innovation can also be seen in two other cases dealing with new devices that allowed consumers to use copyrighted content in ways that had not previously been technologically possible. One of the most celebrated cases in the history of copyright law is the 1984 case of *Sony Corp. of America v. Universal City Studios*.[6] In that case, leading movie studios blamed Sony for copyright infringement being committed with its Betamax VCR. In a five-to-four decision, the Supreme Court sided with Sony, concluding that, although some Betamax users *were* breaking the law by creating personal libraries of recorded movies, Sony was not liable for that

infringement. Not only was Sony not profiting from the infringement, the Court found, but VCRs also had "substantial non-infringing uses," such as "time shifting"—recording a show during the day for viewing in the evening. The Supreme Court held that companies may develop products that have both legitimate and illegitimate uses without triggering copyright liability. The *Sony* decision buoyed the consumer electronics industry, which could develop new media products without fear of ruinous lawsuits should some of their customers misuse their products.

Drawing on the *Sony* precedent, the Ninth Circuit Court of Appeals upheld another breakthrough invention, the MP3 player, in the 1999 case of *RIAA v. Diamond Multimedia*.[7] The Ninth Circuit's decision focused on the 1992 Audio Home Recording Act,[8] which requires that "digital audio recording devices" have copy-protection mechanisms. The court found that Diamond's MP3 player, the Rio, was not a digital audio recording device, as defined by the act, because it merely received music files from a computer, which is not itself a digital audio recording device within the meaning of the act. Moreover, it said, "The Rio's operation is entirely consistent with the act's main purpose—the facilitation of personal use. . . . The Rio merely makes copies in order to render portable, or 'space-shift,' those files that already reside on a user's hard drive."[9] That decision made possible the thriving market for portable music players that is now dominated by Apple's iPod.

File Sharing

It is sobering that Diamond lost in district court before the Ninth Circuit overturned the decision. Had the Ninth Circuit seen the matter differently, technologists and music lovers would today be looking back wistfully at the MP3 revolution that never was, and Apple might never have unleashed the iPod on a world of hip young technology users.

The courts have hardly had an "anything goes" attitude toward new technologies that threaten the interests of copyright holders. The courts have consistently ruled against companies that build business plans around copyright infringement. In 2001 Napster, the leading "peer-to-peer" file-sharing service, was shut down after it was unable to prevent rampant piracy on its network.[10] Napster had argued that it should not be held responsible for the files traded by its users, since it had not reviewed or approved them. The judge rejected that argument, holding that because Napster was built around a centralized database of songs available for download, and because it had been informed of the rampant infringement occurring on its network, it had the ability and the obligation to police that infringement.

In the wake of Napster's downfall, a new breed of peer-to-peer clients sought to avoid Napster's fate by eliminating its Achilles' heel—the centralized database. They designed their networks to be entirely decentralized, so that no file information at all would pass through their servers. Two of the companies, StreamCast Networks and Grokster, prevailed in the Ninth Circuit Court of Appeals,[11] only to have the decision overturned by a unanimous Supreme Court. In *MGM v. Grokster*,[12] handed down last year, the high court held that it was the companies' business models—not their technological design as such—that made them liable for contributory copyright infringement. They noted that the companies' advertisements and internal documents showed a clear intention to promote piracy as a way of increasing ad revenue.

The 2000 decision in *UMG Recordings v. MP3.com*.[13] illustrates that, if anything, the scales of justice were already tilted in favor of copyright holders even when they did not use the DMCA. My.MP3.com was an online service that allowed users to "space shift" their legally purchased CDs by streaming them to other computers over the Internet. The recording industry charged that transmitting copyrighted songs without the permission of the copyright holder was illegal, even if the songs were transmitted only to those who had already purchased the songs on CD. The federal district court was unpersuaded by MP3.com's argument that space shifting was a fair use under copyright law and ruled against the company.[14] It is possible that the decision would have been

The courts have hardly had an "anything goes" attitude toward new technologies that threaten the interests of copyright holders.

overturned by a higher court, as was the *Diamond* case, but MP3.com settled out of court before the case could be appealed.[15]

Fair Use

No area of copyright law better illustrates the capacity of the courts to develop balanced rules than fair use. A central concept in the *Sony*, *Sega*, *Diamond*, and *MP3.com* cases, the fair use doctrine has been a part of Anglo-American law for centuries,[16] but Congress first codified it in the 1976 Copyright Act. Traditionally, fair use protected the right to excerpt printed works for such uses as "criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research" and for creating parodies.[17]

Our culture would be impoverished without fair use.

Our culture would be impoverished without fair use. Consider the story of documentary filmmaker Jon Else, as recounted by Stanford professor Larry Lessig in *Free Culture*.[18] While making a movie, Else taped a scene that happened to include a television in the background. The television was playing an episode of *The Simpsons*. Although this use of the *Simpsons* clip (which was four and a half seconds long) would likely qualify as fair use, the filmmaker decided to play it safe and seek permission to include the shot in his documentary.

He contacted *Simpsons* creator Matt Groening, who gave his permission but told Else to double-check with Fox, the company that produces the program. When he asked Fox, he was informed that permission would cost him $10,000. Otherwise, Fox warned, it might sue Else for copyright infringement.

Else would probably have won in court, but he couldn't afford the expense and didn't need the headache of a legal battle. So instead he digitally edited *The Simpsons* out of the shot and published his movie.

Although fair use failed Else, his story illustrates why the concept is so important. Without it, everyone who makes even trivial or innocuous uses of copyrighted materials would be placed in Else's position. Book reviewers and bloggers would need permission before they could quote other people's writings. College students and library patrons would need to ask permission before photocopying even a single page of a book for later study.

Fair use recognizes that not all unauthorized copies are detrimental to copyright's goal of encouraging creativity. It carves out a zone of autonomy that allows consumers to make copies in cases in which the financial harm to the copyright holder is small but the public benefit of the use might be large. Fair use protects our culture from being overrun by lawyers.

The courts have held that the fair use exception applies in high-tech settings as well. The *Sony* decision was an early step in that direction because it allowed the copying necessary for "time shifting" as a fair use. In the 2003 case of *Kelly v. Arriba-Soft*,[19] the Ninth Circuit considered whether the creation of "thumbnails" of copyrighted images for use in a search engine is a fair use. The court quoted the Supreme Court's 1994 decision in *Campbell v. Acuff-Rose Music*,[20] in which Justice Souter wrote of fair use:

> The central purpose of this investigation is to see whether the new work merely supersedes the objects of the original creation, or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message; it asks, in other words, whether and to what extent the new work is transformative.[21]

Thumbnails used in a search engine, the Ninth Circuit held in *Arriba-Soft*, have a "further purpose" and "different character" than do the copyrighted images on which they are based. They do not harm the market for the original photographs but instead derive their value primarily from the creativity of the search engine's programmers. In short, their use is "transformative," and therefore fair.

The fair use doctrine will be increasingly important to high-tech copyright law as judges are confronted with more and more technologies that manipulate copyrighted content in ways not envisioned by policymakers. It is vital

that the courts continue to exercise judgment in those difficult cases and that they continue to recognize that the fundamental purpose of copyright law is more subtle than simply prohibiting any unauthorized copying of protected works. Rather, as the Constitution says, it is to "promote the progress of science and the useful arts."[22] The question is, Does the DMCA hurt or hinder that progress?

The Digital Millennium Copyright Act

From the time of the Founding until the late 20th century, copyright law primarily implicated centralized, capital-intensive communication technologies. In 1790, when George Washington signed the first copyright act, policing piracy was a relatively simple matter. Only a small minority of Americans could afford to own a printing press, and, when serious infringement occurred, it was generally easy to locate the culprit and bring him to justice.

The 20th century brought new media technologies—the phonograph, the television, and the videocassette recorder—but the economic reality of capital-intensive media remained. Until the 1990s the average American lacked the equipment to mass produce records or videotapes, and, even if he could produce them, covert distribution was difficult and expensive. Moreover, the duplication technologies available to consumers produced poor-quality copies. A duplicate VHS videotape produced on a consumer VCR is of noticeably lower quality than the original.

Two technological developments changed all that. The first was the rise of digital media. Digital music arrived with the compact disc in 1983, and mainstream digital video arrived in 1996 with the DVD. Because computers represent all data as 1s and 0s, they make perfect copies. As a result, pirated music albums or movies—even those produced on ordinary consumer equipment—will look and sound exactly like the originals.

Even more momentous was the rise of the Internet, which allows rapid, decentralized data distribution. Shipping a carton of bootleg videotapes across state lines is expensive, time-consuming, and legally risky. Uploading a bootleg movie to a file-sharing network, in contrast, costs almost nothing, can be done in minutes, and is unlikely to lead to jail time. In the Internet age, people can infringe copyright from the comfort of their homes.

The music and movie industries viewed those trends with alarm. They understood that policing piracy would become much more difficult and that pirated material would become more appealing because the quality would be higher. By the 1990s many copyright holders feared that the existing protections for copyrighted works were insufficient.

The War on Piracy

In their fight against piracy, Hollywood and the music industry employ three principal weapons. The first weapon is the lawsuit. As previously discussed, the Recording Industry Association of America targeted companies that facilitated copyright infringement, including Napster, Grokster, and StreamCast. In 2003 the RIAA began suing individuals as well.[23] It has filed hundreds of lawsuits a month, settling most cases for a few thousand dollars each.[24]

The second weapon is a PR offensive designed to raise public awareness of the costs of piracy. The industry seems to recognize that it can't sue everyone who uses a peer-to-peer network, so it hopes to persuade ordinary consumers that downloading copyrighted materials without paying for them isn't just illegal, it's also wrong. The movie industry has begun running a series of "respect copyright" commercials in movie theaters across the country. Those commercials describe how movie piracy harms ordinary, behind-the-scenes people involved in creating Hollywood movies.[25]

The third industry weapon is digital rights management technology. For example, most commercial DVDs use the Content Scrambling System, an encryption standard designed to prevent unauthorized devices from playing DVDs. The music industry licenses its songs to download services like Apple's iTunes Music

In the Internet age, people can infringe copyright from the comfort of their homes.

Within months of the introduction of any new DRM technology, hackers develop software to circumvent it.

Store, which includes DRM functionality that limits how songs can be accessed and copied. Microsoft's Windows Media format, which is used by many of Apple's competitors in the music download market, includes DRM functionality as well. Those technologies make copying more difficult for the average consumer—digital fences make trespassing harder.

Anti-Circumvention

Unfortunately for the industry, there is no such thing as perfect copy protection. Within months of the introduction of any new DRM technology, hackers develop software to circumvent it. That software is inevitably made available on the Internet.[26] So the industry sought to strengthen this third weapon with extra help from the government. It lobbied Congress for legislation giving copyright holders new powers to prevent circumvention of their copy-protection schemes.

Congress obliged by enacting the Digital Millennium Copyright Act in 1998. Section 1201 of the act prohibits circumventing a copy-protection measure that "controls access to a work" or "protects a right of a copyright owner."[27] It also prohibits creating or trafficking in circumvention tools.[28] In addition to civil remedies, the law imposes criminal fines of up to half a million dollars and five years in jail for violating the provisions "willfully and for purposes of commercial advantage or private financial gain."[29]

Congress was obviously concerned about whether the DMCA would stifle legitimate uses of digital media. The act contains numerous exceptions and exemptions to the general anti-circumvention rule. It exempts circumvention by users who are "adversely affected by virtue of such prohibition in their ability to make noninfringing uses," and it instructs the librarian of Congress to make a list of such uses every three years.[30] The librarian has engaged in two such rounds of rulemaking—in 2000 and 2003. The rules released in 2003 exempt four narrow classes of circumvention, including screen-reading tools for blind users of Adobe's eBook format.[31] The act also specifically permits libraries and educational institutions to circumvent in order to "make a good faith determination of whether to acquire a copy."[32]

None of those exemptions applies to the prohibitions on creating or trafficking in circumvention tools. That means that users are allowed to circumvent copy protection, but they cannot help others to do so. Since most users lack the technological sophistication to write circumvention tools for themselves, that renders those exemptions practically irrelevant. How likely, for example, is the average blind person to know how to write her own screen-reading software? Of what use are the exceptions if the law makes anyone who "trafficks in" such software—i.e., sells it to a blind person—a felon?

The act grants exemptions for security testing and encryption research on computer programs. Perhaps the most important exception concerns reverse engineering. It allows circumvention for the purpose of "identifying and analyzing those elements of [a] program that are necessary to achieve interoperability."[33] Moreover, it allows the distribution of reverse-engineering tools for that purpose and "for the purpose of enabling interoperability of an independently created computer program with other programs."[34]

Although well-intentioned, the reverse-engineering exception is too vague to offer meaningful protection for innovators seeking to build compatible products. To be effective, a DRM scheme must prevent unauthorized devices from "interoperating" with it. Because unauthorized devices are not bound to enforce the rules of the DRM system, the designer of a DRM system cannot afford to allow them access to protected content. By definition, then, any product that achieves interoperability against the wishes of the creator of another product is "circumventing" the DRM scheme.

Yet, strangely, the statute gives no clear guidance on how to distinguish "enabling interoperability of an independently created computer program" (which is permitted) from "circumvent[ing] a technological measure" (which is prohibited). Later in this paper, for example, I

discuss the case of the Streambox VCR, a product designed to interoperate with Real's products for streaming video over the Internet. The case was settled out of court after Streambox lost the first round, so we will never know if the courts would have recognized this as an example of legally protected reverse engineering. But we do know that the exception wasn't sufficient to protect the company from being forced to withdraw the product under the threat of a ruinous lawsuit.

Entrepreneurs are seldom interested in adding legal risk to the technological and market risks they already face. As long as the precise scope of the reverse-engineering exception remains murky, most small developers will decline to exercise it out of fear that their products might be declared illegal in the future. A theoretical right to reverse engineer is useless if it is not backed up with clear precedents establishing what is and is not legal. So far, such precedents are sorely lacking.

Copyright Law Goes beyond Copyright

The existence of so many ad hoc exceptions should make us wonder if there might be fundamental flaws with the DMCA's general approach to combating piracy. Coupling a sweeping prohibition with a long list of narrow exceptions is a poor way to draft legislation. If security testers, encryption researchers, the blind, and libraries all have legitimate reasons to circumvent, might there be other legitimate reasons that Congress did not think of? Should people with other legitimate reasons to circumvent be subject to the whims of the librarian of Congress?

The anti-circumvention rule requires so many exceptions because it is a dramatic expansion of the rights of copyright holders. In effect, the DMCA creates an anti-circumvention right that is materially different from and much more sweeping than the underlying copyright. Aside from the exceptions noted above, *any* tampering with DRM systems—even tampering that does not infringe copyright—is illegal. DRM systems and the DMCA give copyright holders much greater control over their products and their customers than they have ever enjoyed under traditional copyright law.[35]

A traditional book publisher, for example, cannot use copyright law to limit how many photocopies a reader can make for personal use, where the book can be read, or what brand of reading glasses the user may use when reading the book. Yet, thanks to the DRM technologies and the anti-circumvention restrictions that give them legal force, intellectual property holders in the digital realm have both the technological ability and the legal right to place such restrictions on their customers. The publisher of an Adobe eBook, for example, may limit how much of the book can be printed, whether text can be cut and pasted into another application, and whether the software may read the text aloud. The publisher may also prevent users from "lending" or "giving" the book to another person and may set an expiration date for the eBook, after which it would be unreadable.

Many of those actions, such as cutting and pasting excerpts into a book review or printing a copy of an eBook for personal use, qualify as fair use under traditional copyright law. Nevertheless, the DMCA makes it illegal for anyone to "circumvent" Adobe's controls in order to exercise fair use. That has the practical effect of dramatically broadening the scope of digital copyrights and narrowing the freedom of individuals to use content they have legally purchased.

The same trends are evident in the music industry. The purchaser of an audio CD can play the CD on any CD player she likes. She can also "rip" the songs onto her computer for transfer to the portable music player of her choice. Songs downloaded from Apple's iTunes Music Store are not nearly as flexible. They can only be played using Apple software, and they may not be transferred to any portable music player other than an iPod. A user who wishes to listen to music with a non-Apple product must violate the law to transfer any music she purchased at the iTunes Music Store directly to a non-Apple player.[36]

To qualify for protection under the DMCA, a DRM scheme must be designed to "effectively control access" to copyrighted works.[37]

In effect, the DMCA creates an anti-circumvention right that is much more sweeping than the underlying copyright.

But there is no requirement that a DRM system be limited to that purpose. DRM systems may limit access to both copyrighted and noncopyrighted material, and they may place any restrictions they like on access, regardless of whether those restrictions are necessary to prevent piracy. Thus, if a compilation of recorded song performances protected by a DRM system has some selections that are copyrighted and others that are in the public domain, it is a violation of federal law to circumvent the system even to access the material in the public domain.

It seems unlikely that Congress intended to give the creators of digital media technologies broad powers to control how their products are used, but that has been a major effect of the law. The DMCA's anti-circumvention provisions extend the power of copyright holders well beyond copyright protection.

A Copyright-Based Home Video Cartel?

Recall how IBM tried to capture the market for computers compatible with its popular PC through the copyright on its BIOS. Happily, the courts nurtured the practice of clean room reverse engineering so that a compatible BIOS could be written without infringing IBM's copyright. Today many successors to IBM compete to build cheaper and more powerful desktop and laptop computers, all to the good for consumers and small businesses. If software reverse-engineering methods had not been sheltered by the courts, IBM might have used its copyright on the BIOS to thwart competition and maintain dominance in the business PC market to this day.

The anti-circumvention provisions of the DMCA threaten innovation and competition in all digital industries the same way. The DMCA's effects can best be illustrated by recent developments in consumer video.

DRM systems may limit access to both copyrighted and noncopyrighted material, and they may place any restrictions they like on access.

Copyright Used to Control Playback Functions

The climate for consumer video products has been transformed since the Supreme Court allowed the sale of VCRs (as a practical matter) in 1984. The VCR made its way into nearly every home and enjoyed a long reign. But after 15 years in the limelight, it was upstaged by the DVD, which was launched in 1996.

The new format includes many features sought by Hollywood. One is known as "region encoding." The DVD format's designers segmented the worldwide DVD market into "regions,"—the United States and Canada, for example, make up "region one."[38] To prevent resale across regions, each DVD is marked with a "region code," and a DVD player will play only DVDs encoded for its region. That allows the industry to charge higher prices in the United States and lower prices in India without worrying about the Indian version being resold in the United States. And it lets Hollywood release a movie over the summer in the United States and at Christmas in Europe, thus preventing sales of the American DVD from undermining the summer market for movie tickets in Europe.

The DVD format also allows DVD publishers to place other restrictions on their customers. For example, many movies on DVD are preceded by commercials. Publishers can prohibit viewers from fast-forwarding through those commercials. Viewers who press the "fast forward" button on their remotes are informed that they are "not allowed" to use the fast-forward feature at that time.[39]

Needless to say, many consumers find those restrictions annoying. Surely a consumer electronics company that produced a DVD player without such "features" would have a competitive advantage in the marketplace.

That's where the DMCA comes in. Most commercial DVDs use a proprietary encryption technology known as the Content Scrambling System to deter piracy. In order to make a DVD player that will play CSS-encrypted DVDs, a company needs to seek the certification of the DVD Copy Control Association, the industry consortium that created the DVD standard.[40] The consortium requires that DVD players respect region cod-

ing and fast-forwarding restrictions. If a manufacturer reverse engineered CSS and created an unauthorized DVD player, it would likely be sued for violating the anti-circumvention provisions of the DMCA.

Such a lawsuit might have nothing to do with piracy. Watching a British DVD in the United States is not an act of piracy any more than is listening to a Canadian CD or reading an Austrialian book. Yet the DMCA does not draw such distinctions. Any "circumvention" of the DVD encryption system—even for purposes that are otherwise perfectly legal—is against the law.

The movie industry has every right to segment the worldwide market for DVDs, but it should bear the costs of doing so. Those costs might include requiring no-resale contracts with distributors and monitoring sales in low-price countries to make sure DVDs were not being resold outside their intended market. Deciding whether those costs would be worthwhile might be difficult. The industry's desire for market segmentation is not, however, a good reason to outlaw the sale of unofficial DVD players. The role of government is not to ensure that a private business's pricing strategy succeeds, and consumers, who have not agreed to help enforce the DVD cartel's segmentation scheme, are under no obligation to respect it.

Other industries that employ price discrimination schemes routinely bear such costs. Manufacturers of nonperishable consumer goods like cereal and shampoo, for example, fight a perpetual battle with "diverters" who undermine their market segmentation schemes by reselling their products. The courts have consistently held that, absent specific evidence of fraud or breach of contract, such diversion is perfectly legal.[41] And, despite repeated lobbying, Congress has refused to enact legislation to make it easier for manufacturers to prevent such diversion.[42]

It is hard to see why Congress should give the DVD format's restrictions on fast-forwarding the force of law. Yet the anti-circumvention provisions of the DMCA do precisely that.

Copyright Used to Control Playback Devices

The practical legal control the movie industry exercises over playback may be a modest annoyance for most users, but users of the Linux operating system have particular reason to be upset. The DVD CCA has yet to approve any software DVD players that would work on computers that run the Linux operating system. Frustrated by the industry's neglect of their beloved operating system, open-source developers created a program called DeCSS in October 1999. It removes the encryption from DVDs, allowing them to be played by generic video-playing software.[43]

DeCSS clearly has substantial noninfringing uses—playing legally purchased DVDs, for example—and would almost certainly have been found legal under the Supreme Court's decision in the *Sony* case. But when *2600* magazine published the program on its website, the Motion Picture Association of America sued under the freshly enacted DMCA. In 2001 the Second Circuit Court of Appeals ruled that the magazine could not publish or even link to copies of the program because it was an illegal circumvention device.[44]

Today the option to play DVDs under Linux remains under a legal cloud. Open-source DVD players are widely available on the Internet, but they all require "circumvention" software (which is theoretically illegal in the United States) in order to play commercial DVDs. A successor to DeCSS, called libdvdcss, has been created by non-American programmers. But to avoid legal trouble, most developers of video software require that the libdvdcss library be downloaded and installed separately—a cumbersome and confusing process for novice users.

The movie industry has not chosen to pursue or prosecute the developers, distributors, or users of libdvdcss, perhaps because of the negative publicity generated by the DeCSS prosecution. But the legal uncertainty surrounding DVD playing remains a serious problem for the American Linux community. Linux developers in the United States are likely to avoid writing DVD soft-

The role of government is not to ensure that a private business's pricing strategy succeeds.

Any American who watches a DVD on a Linux computer is guilty of a federal crime.

ware for fear of legal trouble. And, strictly speaking, any American who watches a DVD on a Linux computer is guilty of a federal crime. It's not fair to have this threat hanging over the heads of Linux users, even if they're unlikely to be prosecuted.

Did banning DeCSS at least make it more difficult to pirate movies? There's little reason to think so. The CSS system prevents *playback* of DVD movies, but it does nothing to prevent duplication of the scrambled data. A pirate can make a perfect copy of a scrambled DVD without ever cracking its encryption. No circumvention software is needed to download CSS-scrambled video, burn it to a DVD-R disc, and play it in any consumer DVD player.

Of course, in practice, pirates don't usually distribute movies in CSS-scrambled format. What commonly occurs is that one person, perhaps outside the United States, unscrambles a DVD and uploads the unrestricted file to a peer-to-peer network. Once an unrestricted movie file has been made available, those who download it can watch it without any circumvention tools. So unless you can prevent the uploader from getting his hands on DeCSS—a task that has proven impossible in practice—CSS will do nothing to deter those who download bootleg movies from peer-to-peer networks. In practice, the only significant effect of the DeCSS ban has been to inconvenience the movie industry's legitimate customers.

DVD: The Next Generation

Plans are now on the drawing board for the Blue-Ray Disc, which, its backers hope, will replace the DVD as the new standard for home video. Last summer the Blue-Ray Disc Association announced that Blue-Ray Discs would include a number of "security" technologies designed to deter piracy. For example, the ROM Mark will be a difficult-to-forge holographic identifier that will ensure that Blue-Ray players will play only authorized discs. Even more ambitious is BD+, a system that will allow video players found to be vulnerable to circumvention to be rendered unable to play new releases until their software has been "upgraded" to the Blue-Ray consortium's satisfaction.[45]

If Blue-Ray, or something like it, became a universal standard, the consortium that controls the standard would have control over who could produce home video players and what features they could have. That control would be backed by the legal authority of the DMCA, rather than developed in, and constantly subject to, competition to provide the players and features that consumers want most. Not only could it decline to approve video products, as the DVD CCA did to software Linux players, Blue-Ray could use BD+ to revoke the encryption keys of products already on the market, rendering them inoperable. Manufacturers who refused to comply with the consortium's rules could simply be frozen out of the market.

Copyright Control Metastasizes

If the features available on playback devices—and, indeed, the devices themselves—are too subject to control by content owners who have used the DMCA to bootstrap copyrights into control of the entire media experience, there must be an alternative platform. Consumers can turn to cable. Perhaps, if they have to, they can get the entertainment they want streamed over the Internet.

Alas, the same trends toward restricting market access and dictating product functionality can be seen in current battles over next-generation cable television standards and streamed Internet content. Those trends, too, are attributable to the DMCA's anti-circumvention provisions.

Video over Broadband

Hoping to save consumers money and to increase competition by eliminating the need for the "set-top box" that now sits atop the TV of almost every cable customer,[46] the Federal Communications Commission has required cable TV operators to support the Cable-

CARD, a credit card–sized device that allows digital TVs to unscramble TV channels. The CableCARD is part of the OpenCable platform, which was developed by a cable industry consortium called CableLabs.[47]

OpenCable-compliant devices are required to include DRM features that limit how CableCARD content can be used.[48] The system is designed to prevent unauthorized devices from gaining access to the video stream so that it cannot be converted into open formats and redistributed on the Internet. Of course, any device that "circumvents" those copy protections to access the video stream without authorization would violate section 1201 of the Digital Millennium Copyright Act. Here, again, an incumbent industry consortium is using the DMCA to control the capabilities and the devices consumers may use to view content.

The first-generation cable card, released in 2004, is "one way." That is, it can receive video streams, but it cannot manage the two-way communications necessary to access high-tech features like video-on-demand and interactive programming guides. Negotiations over the specifications for the two-way CableCARD, which is slated to be released later this year, have dragged on for some time. The cable industry is intent on maintaining control over the "look and feel" of the customer experience.

Companies building devices to improve the consumer video experience have accused the industry of deliberately dragging its feet to avoid having to relinquish control. In an angry January 18, 2005, letter to the FCC, Matthew Zinn, general counsel to TiVo, a leading innovator of digital video recorders, wrote:

> There is little doubt that [the cable industry] would support two-way CableCARD products from manufacturers such as Samsung and LG Electronics as long as those products run [the OpenCable Applications Platform] and look, feel, operate, and are controlled by cable operators in every way. Such products, however, do not provide consumers with a *competitive* alternative to operator-supplied integrated set-top boxes. They don't offer consumers additional innovative services and features. All they do is provide consumers with a choice between leasing a box from cable or buying essentially the very same box from Samsung or LG Electronics. In other words, you can lease a Honda Accord from your cable operator or you can buy a Honda Accord.[49]

Just two months later, TiVo apparently decided that hawking Honda Accords wasn't such a bad business after all. It signed an agreement with Comcast to provide TiVo-branded services to Comcast subscribers. News reports at the time cited "investor concerns over the digital video recorder pioneer's future."[50] If TiVo had failed to find a partner among the major cable companies, it might have struggled to stay in business. This is not so much because of competitive pressures as because of a legal environment in which access to television content is increasingly limited to devices that have been specifically licensed by the cable industry.

How has that affected TiVo's behavior in the marketplace? In November 2005 TiVo announced a deal with Yahoo! to provide Yahoo! content via TiVo's set-top boxes. A *New York Times* story by Saul Hansell reported that Yahoo! would provide television listings, photos, weather, and some interactive features.[51] However, despite the fact that Yahoo! was "actively developing" video programming, no video content was included in the agreement. Why not? Hansell suggests that TiVo was "caught in the middle" because it "depends on the very companies this technology bypasses." If companies could transmit video content directly to consumers via set-top boxes like TiVo's, Comcast's premium cable content would no longer have a leg up in the homes of its millions of subscribers.

If it weren't for the DMCA, TiVo could afford to take a much stronger stance when negotiating with the cable industry. TiVo would know that, if negotiations broke down, it always had the option of reverse engineering

Access to television content is increasingly limited to devices that have been specifically licensed by the cable industry.

Innovation occurs precisely when an old technology is used in a new way not envisioned by its original designers.

the CableCARD and selling its product directly to consumers. The DMCA changes that dynamic. TiVo cannot produce a video device that accesses cable content without the permission of CableLabs. If it did, the device would likely be declared a circumvention device under the DMCA. And without the ability to access cable content, TiVo's box would be practically useless to many of its customers. As a result, TiVo simply cannot afford to alienate the cable industry.

One wonders what innovative services and features TiVo might have developed if it had had the option of offering a genuinely independent alternative to the cable industry's products. We will probably never find out. With TiVo's revenues dependent on access to cable customers, the company is unlikely to produce any products—such as direct Internet downloading of video—that might threaten TiVo's partners' business model.

Innovation occurs precisely when an old technology is used in a new way not envisioned by its original designers. Revolutionary technologies are disruptive, and they often threaten industry incumbents. Had a technology like the CableCARD been in place in the early 1980s, it is unlikely that the first VCRs would have gotten industry approval. The issue would never have reached the Supreme Court because the industry would have simply declined to approve the device, with copyright law's legal monopoly operating murkily in the background rather than front and center as it did in the *Sony* decision. The growing cartelization of the consumer video marketplace ought to worry anyone who values vigorous competition. Through the anti-circumvention provisions of the DMCA, the federal government has given incumbent content industries too much power over the design of new media technologies.

Perhaps worst of all, the CableLabs certification process completely freezes out amateur video hobbyists and the users of open-source tools. The OpenCable specification is hundreds of pages long, and the certification process takes months. Electronics buffs who want to build their own video devices will simply be unable to do so without breaking the law. And, as with DVDs, users of Linux and other open-source operating systems will be unable to legally watch or record cable television programs with their computers, though to do so would violate no copyright.

It is impossible to predict how those restrictions might affect the future of innovation in consumer video technology. But granting a single body the power to decide who may produce video products and what features those products may have is certainly not a recipe for a vibrant consumer electronics industry. The DMCA and the FCC's mandates give CableLabs a quasi-governmental authority over the video marketplace. Given that CableLabs is composed of cable industry incumbents with a vested interest in preserving the status quo, there is little reason to think the consortium will be sympathetic to technological innovations that might undermine its members' current market positions.

The same is true of the numerous other copy-protection schemes being built into virtually every home entertainment device on the market. The latest DRM schemes require that participating consumer electronics manufacturers comply with hundreds of pages of rules about what approved devices may and may not do with protected content. Complying with all those requirements is simply impossible for individuals who just want to tinker with the latest technologies to find out how they work and perhaps invent something better.

Internet Video Streaming

We take for granted that any analog audio device can be plugged into any other analog device and work correctly. You can use the same pair of headphones with any stereo, tape deck, Walkman, computer, or other device with a standard 3.5-mm headphone jack. Any device with an audio output will work with any device with an audio input even if their manufacturers have never heard of each other. The same is true of analog video: any TV can be attached to any VCR, TiVo, PlayStation, XBox, or camcorder using

standard connectors and the devices will be able to communicate.

Devices work together because they have been designed to conform to open standards. Any device that follows the rules for a 3.5-mm headphone jack is guaranteed to work with all the other devices that follow the same rules. Not only is that extremely convenient for users, who do not have to worry about compatibility, but it has economic benefits as well. It allows specialization and economies of scale. Consumers can reuse devices: the headphones they purchased for an iPod can also be used with a laptop or a tape player. And it reduces development and testing costs because manufacturers do not have to test for compatibility with every product on the market. As long as a device is built to the standard and compatibility has been tested with a handful of products, the manufacturer can be certain that it will work with other products the manufacturer may never have even contemplated.

The same principle applies to software. Indeed, the Internet itself would be impossible without open standards: the TCP/IP protocol that serves as the "plumbing" of the Internet is an open standard.[52] Every device that connects to the Internet conforms to the standard, ensuring that it will be able to talk to all the other devices.

The most successful online applications use open standards as well. The World Wide Web, for example, is built on two open standards: HTTP[53] (which governs how clients and servers communicate with each other) and HTML[54] (which describes how Web content is displayed on the user's screen). E-mail, too, is built on open standards. Mail servers communicate using the SMTP[55] protocol, and e-mail clients like Outlook and Eudora use open standards like POP3 and IMAP to retrieve mail from e-mail servers.

All of those open standards are available for everyone to use. The developer of a new Web browser would need only to comply with the requirements of HTTP and HTML and his new browser would be compatible with the other Web servers and Web browsers on the market.[56]

Unfortunately, open standards have not caught on for every Internet application. To see what happens when companies try to get by with proprietary standards, consider the case of streaming video.

More than a decade after the first streaming video products appeared, the leading products are disappointing. There are three major video platforms owned, respectively, by Real, Microsoft, and Apple.[57] None is compatible with the others. In offering streaming media services, webmasters must choose which of those formats to support. Streaming software has improved relatively slowly, in part because there is so little competition. Although the formats do compete against one another, there is no competition for software within each format. Users wanting to view a Real stream, for example, may do so only with Real's player, not with the Apple or Microsoft video players. A new firm seeking to enter the market for streaming video software cannot simply produce a better video player. It must also design a new video format, create a new server program, and convince content providers to adopt the format. That is beyond the capacity of all but the largest software companies. As a result, with one exception,[58] there have been no significant new entrants to the market in nearly a decade.

What prevents companies or open-source projects from producing streaming video products compatible with existing protocols? The reasons are complex, but the DMCA is clearly one of the culprits. Consider the case of the Streambox VCR. Developed in the late 1990s, it was software that could record video streams encoded in Real's video format and save them to the user's hard drive. When it was released, Real sued Streambox and received a preliminary injunction against its distribution.[59] A few months later, Streambox settled, agreeing to remove the recording functionality of the VCR and pay undisclosed damages.[60]

Granting the preliminary injunction,[61] the district court accurately noted that the Streambox VCR circumvents a copy-protection measure. Real's streaming video format had a "copy switch" that allowed content owners to determine whether users could

More than a decade after the first streaming video products appeared, the leading products are disappointing.

save the stream to their hard drives. The RealPlayer allowed users to save a video stream only if the owner of the player had enabled the copy switch. The Streambox VCR, in contrast, ignored the switch, allowing users to save files even if the copy switch was turned off.

Streambox likely named its product the Streambox VCR in reference to the 1984 *Sony v. Universal Studios* decision, which explicitly held that consumers *do* have some fair use rights to use copyrighted content in ways not envisioned or approved by the copyright holder.[62] But in practice, that principle does not apply where DRM technologies are concerned. The fair use right to "time shift" and "space shift" streaming video content is of little use because, under the DMCA, any device that would do that is illegal.

Indeed, it is not clear whether *any* unauthorized player of Real video streams could pass muster under the DMCA. On the one hand, any player would need to fake the "secret handshake" that the RealServer uses to verify that it is connecting to a RealPlayer. The mere act of faking the secret handshake might be an illegal circumvention. On the other hand, the reverse-engineering exception might apply in a case like this one, since the clear purpose of faking the secret handshake would be to enable interoperability among computer programs. The precedents thus far give little hint as to which kinds of circumvention would qualify for the reverse-engineering exemption and which would not.

That uncertainty presents a serious problem to any entrepreneur thinking about producing a competing video player for Real streams. Any product he developed might be declared an illegal circumvention device and be forced off the market. Even if he had a strong case, Real has deep pockets, and so the entrepreneur's venture capital might run out before he could vindicate his (potential future customers') rights.

A new entrant would also face a deeper problem: he would have to be very careful about what features he added to his product. If he made a player that worked precisely the same way that Real's player does, it is possible that he could prevail in court by arguing he had not "circumvented" a technical measure but merely implemented it precisely as Real intended. But any feature that allows the user to store, convert, or manipulate video content in a way not permitted by the RealPlayer would strengthen the charge that his product was a "circumvention device." That creates a dilemma: if his product had no features not found in the original product, how could he differentiate himself and attract customers?

In virtually every category of media, the anti-circumvention provisions of the DMCA are vesting incumbents with broad powers to dictate the forms in which consumers can view copyrighted content and the devices they can use. Entire classes of devices, like those running on the Linux operating system, are being excluded from the provision of popular media to consumers. The consumer-serving innovations lost to this DMCA lockup cannot be known, but, judging by the results in other technology markets that have remained competitive, like that for the PC, the losses are substantial.

The precedents thus far give little hint as to which kinds of circumvention would qualify for the reverse-engineering.

DMCA Abuse

The full extent of the DMCA's chilling effect on competition is revealed by some of the most outrageous examples of opportunistic companies misusing the DMCA to stymie competitors. Although none of the examples that follow resulted in favorable verdicts for the plaintiffs, they illustrate just how ripe for abuse the law is. The DMCA's anti-circumvention provisions are a continuing invitation to companies that wish to thwart competitors using nonmarket tools.

The Lexmark Case

Printer maker Lexmark sells its "prebate" toner cartridges with special software that prevents companies other than Lexmark from refilling them. Static Control Components, a competing company, reverse engineered Lexmark's printer cartridges in order to defeat those restric-

tions. That would obviously serve consumers because the entry of SCC and other competitors would force Lexmark into price and quality competition in the cartridge refill market. No law should interfere with such beneficial competition. But, in December 2002, Lexmark sued SCC under the DMCA, alleging that the company's chips gain "unauthorized access" to the printer.[63]

The Sixth Circuit Court of Appeals thought Lexmark's argument a little too clever. It ruled against Lexmark in October 2004, holding that the DMCA protects only "access control measures" that restrict access to copyrighted content. A printer, it held, is not eligible for copyright protection, and therefore accessing its functionality cannot be a violation of the DMCA.[64]

That decision cited a previous decision by the Court of Appeals for the Federal Circuit, *Chamberlain v. Skylink*. The Chamberlain Group, a maker of garage door openers, sued Skylink Technologies, makers of replacement remote controls for Chamberlain's products, under the DMCA for "circumventing" the access control technologies in Chamberlain's garage door openers. In 2003 a district court had granted Skylink summary judgment, ruling that "a homeowner has a legitimate expectation that he or she will be able to access the garage even if the original transmitter is misplaced or malfunctions."[65] The Federal Circuit court upheld the holding.[66]

As heartening as it is that the defendants prevailed in those cases, they were far from harmless. Legal battles are expensive, especially for small defendants who don't have in-house legal teams. Even worse, SCC was prevented from selling its product for 19 months—a major blow to its bottom line. Smaller, less-well-capitalized companies may bow out rather than fight a years-long legal battle to sell a competing product.

There is every reason to expect more frivolous lawsuits in the future. The *Chamberlain* decision rested on the fact that Chamberlain had not attempted to contractually prohibit its customers from using competitors' remote control devices. Had Chamberlain included a license with its products that restricted the use of competing remote controls, the judge said, the case might have had a different outcome.[67]

In his concurrence with the Sixth Circuit's *Lexmark* decision, Judge Gilbert Merritt chastised the court for not taking a clearer stand against such abuse of the DMCA. He urged his colleagues to "make clear that in the future companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods for themselves just by tweaking the facts of this case."[68] Unfortunately, the majority opinion did not contain such strong language, leaving the door open for more of the same.

Using Copyright to Enforce Contracts?

An important wrinkle in the *Lexmark* case is the issue of contractual obligations. As the Sixth Circuit explains in its decision:

> Lexmark markets two types of toner cartridges for its laser printers: "Prebate" and "Non-Prebate." Prebate cartridges are sold to business consumers at an upfront discount. In exchange, consumers agree to use the cartridge just once, then return the empty unit to Lexmark; a "shrink-wrap" agreement on the top of each cartridge box spells out these restrictions and confirms that using the cartridge constitutes acceptance of these terms. Non-Prebate cartridges are sold without any discount, are not subject to any restrictive agreements and may be refilled with toner and reused by the consumer or a third-party remanufacturer.[69]

Under those circumstances, SCC's customers arguably had no right to use SCC's product in the first place, since they agreed to return the prebate cartridges after the first use.

That hardly justified Lexmark's lawsuit, however. The contractual obligations of Lexmark's customers have nothing to do with protecting copyright, the purpose of the DMCA. If Lexmark believed that contracts on its prebate cartridges were being violated, it could have sought remedies under contract law. It would be perverse to allow litigants to

The contractual obligations of Lexmark's customers have nothing to do with protecting copyright, the purpose of the DMCA.

use copyright law to obtain remedies not available to them under the law of contract.

Moreover, Lexmark's prebate agreements are with its customers, not SCC. As a non-party to the prebate contract, SCC is in no way bound by its terms. If Lexmark had had a cause of action against SCC, it would likely have been interference with prospective economic advantage, interference with contractual relations, or some similar business tort. But, again, Lexmark should not have used copyright law to achieve those other ends. The DMCA anti-circumvention provisions are ripe for this kind of creative, competition-chilling lawyering.

Congress ought not to enact specially crafted copyright legislation to assist particular industries in enforcing the terms of their contracts.

The same argument applies to Apple's iTunes Music Store. The iTunes Terms of Service state that users may not "attempt to, or encourage or assist any other person to, circumvent or modify any security technology or software."[70] Songs downloaded from the service come with copy protection, and Apple has aggressively prosecuted hackers who have developed software to "circumvent" that copy protection.

Apple should be free to offer whatever contractual arrangement consumers will accept, including agreements to abide by DRM systems that most consumers would find oppressive. Consumers circumventing the DRM features in iTunes may be violating their contractual obligations. However, that does not justify using copyright law to prohibit third parties from producing circumvention tools for iTunes music. Those third parties are not parties to the Terms of Service and are not bound by its terms.

More to the point, Congress ought not to enact specially crafted copyright legislation to assist particular industries in enforcing the terms of their contracts. If a contract's terms are arbitrary, unreasonable, and impossible to enforce—as the terms of Apple's DRM scheme arguably are—then the company ought to bear the legal and public relations costs that come with monitoring and suing its own customers.

"Click-through" contracts, like the one that all users of Apple's iTunes service must agree to, usually consist of page after page of dense legal jargon. Consumers have gotten in the habit of clicking the "Agree" button on such contracts without reading their terms. Most customers are not even aware of how their rights might be restricted by such contracts.

If Apple wishes to enforce its contracts, the company should enforce them in the open, by bringing lawsuits against customers who violate their terms. If Apple did get in the habit of suing its own customers for playing iTunes songs on other companies' MP3 players, that behavior would likely get a lot of press coverage, and it would make potential iTunes customers think twice about using the service. That, in turn, would make Apple think twice about using litigation to lock its customers into using its products.

Thanks to the DMCA's anti-circumvention provisions, Apple can point its legal guns at third-party developers of circumvention tools rather than compete to please customers. It can prevent its customers from switching to other products without the risk of bad publicity. That hardly seems like a tactic Congress should be enabling.

The Criminal Law Trump Card

The DMCA also gives Apple a club that is never available to parties in ordinary contract disputes: criminal penalties. If Apple reneges on the terms of a contract with its customers, they may sue the company for monetary damages. But no matter how egregious Apple's breach of contract may be, customers cannot have Apple CEO Steve Jobs thrown in jail. Yet Apple *can* ask the federal government to throw those who circumvent its DRM system in jail—even if they never engaged in piracy. The DMCA provides for criminal penalties of up to a half a million dollars and five years in jail the first time someone circumvents a DRM system "willfully and for purposes of commercial advantage or private financial gain." If you work for a company that produces a "circumvention tool"—for example, a Linux DVD player—you could face time in prison, even if you never made a single illegal copy of any DVD.

The first criminal prosecution under the DMCA occurred in 2001. Dmitry Sklyarov, a

Russian programmer, was arrested for developing a program to remove copy-protection features from files in Adobe's eBook format.[71] Sklyarov believed his program was legal in Russia, where it was developed and marketed. Among the uses for which it was marketed was making eBooks compatible with screen-reading software used by the blind. When he presented a talk on the flaws in the eBook format to a conference in the United States in the summer of 2001, he was arrested at the behest of Adobe Systems, makers of eBook software. A week later, after an intense backlash from its customers, Adobe flip-flopped and called for his release.[72]

But the damage had already been done, and Adobe had made its point. The Justice Department continued its prosecution (as Adobe doubtless expected it would), and Sklyarov spent three weeks in jail and another four months out on bail but unable to leave the United States. The charges were finally dropped and he was allowed to return to Russia in December 2001, but only on the condition that he return the following year to testify against his employer, Elcomsoft, in the government's prosecution of that company.[73]

A jury acquitted the company the following year,[74] but the possibility of a five-year jail sentence will still make everyone wary of creating software that might be found to be a circumvention device in court. Criminal penalties are clearly excessive for the enforcement of ordinary contracts, especially when only one party—the customer—is subject to them. Whatever the merits of anti-circumvention law, no one should face long jail sentences for merely creating, distributing, or using a "circumvention tool" that might have uses unrelated to piracy.

Threats to Academic Freedom

Powerful companies have also used the provisions of the DMCA to bully and intimidate researchers who expose flaws in their products. Sklyarov was arrested after giving an academic presentation on the flaws in Adobe's eBook format. Although it's not certain that his presentation prompted the arrest (it's possible that he would have been arrested regardless of his reasons for being in the country), the possibility that the DMCA could be used to squelch criticism of the flaws in software products should be a matter of serious concern.

Another troubling case involves the Secure Digital Music Initiative, an industry consortium charged with developing new technologies for copy protecting digital music. In 2000 SDMI issued a public challenge inviting attempts to break its "digital watermarking" technologies. A team led by Ed Felten, a computer science professor at Princeton University, took up the SDMI challenge and succeeded in breaking the technologies. But when the team decided to present their findings at the International Information Hiding Workshop in 2001, Felten received a letter from the Recording Industry Association of America warning that presentation of the paper could lead to legal action under the DMCA.[75]

Felten pulled his paper from the workshop. Then, with the help of the Electronic Frontier Foundation, he sued the SDMI, the RIAA, and Attorney General John Ashcroft seeking a declaratory judgment that presenting his paper would not violate the DMCA.[76] Faced with a strong legal challenge, the recording industry quickly backed down, insisting that they never intended to prosecute Felten in the first place. He was allowed to present his paper at the USENIX conference later that year.[77]

Similar threats have been made in more recent cases. In July 2002 Hewlett Packard threatened to sue security researchers under the DMCA for publicizing vulnerabilities in its Tru64 operating system.[78] The threat elicited such a backlash among HP's customers that the company quickly backed down.[79] In April 2003 Blackboard, a maker of popular software for classroom collaboration, cited the DMCA when it obtained an injunction preventing two university students from presenting their research on the security flaws in the Blackboard system.[80]

Fear of DMCA prosecution has damaged the image of the United States in the worldwide computer science community. After Sklyarov's arrest, prominent Dutch security researcher

The possibility that the DMCA could be used to squelch criticism of the flaws in software products should be a matter of serious concern.

Fear of DMCA prosecution has damaged the image of the United States in the worldwide computer science community.

Niels Ferguson decided not to publish a paper on the serious flaws he had found in Intel's High Bandwidth Digital Content Protection system, citing fear of prosecution should he ever visit the United States.[81] Alan Cox, one of the world's leading open-source developers whose work on the Linux operating system sometimes involves reverse engineering, resigned from the USENIX committee of the Advanced Computing Systems Association because of worries about traveling to the United States.[82]

Thus far, there have been no judicial rulings upholding censorship of academics under the DMCA. Threats from the likes of HP and the RIAA may be little more than saber rattling. But in an uncertain legal environment threats can be as effective as lawsuits. To protect free speech, we should be skeptical about any law that gives companies the opportunity to threaten those who criticize their products, to say nothing of the loss to consumers, the economy, and society when the weaknesses in technical products cannot be exposed.

What about Piracy?

Some advocates of the DMCA acknowledge that the law isn't perfect but insist that it is necessary to prop up DRM schemes and thereby thwart piracy. Advocates of the DMCA like to paint pictures of anarchy among Internet providers in the absence of DRM technologies. Jack Valenti, who served as the president of the MPAA for 38 years, had this to say about the consequences if Congress didn't mandate the use of the "broadcast flag," a DRM technology that was designed to prevent redistribution of television programs:

> Today, [a movie] is exposed to great peril, especially in the digital environment. If that movie is ambushed early on its [distribution] travels, and then with a click of a mouse, and without authorization, sent hurtling at the speed of light to every nook and cranny of this planet, its value will be seriously demeaned.[83]

Valenti is certainly right that the Internet gives ordinary consumers the power to engage in massive copyright infringement with the click of the mouse. And that is a serious issue. But Valenti is wrong to think that the broadcast flag or other DRM technologies are an effective solution. The fundamental threat to copyright control is the technological capabilities of the Internet itself. DRM strikes at the wrong target.

No one understands that better than Apple CEO Steve Jobs. In a December 2003 interview with *Rolling Stone* magazine, he described the 18-month negotiating process between Apple and the recording industry that led to the iTunes Music Store. He was surprisingly candid about the inevitable failure of copy-protection technologies:

> At first we said: None of this technology that you're talking about's gonna work. We have Ph.D.'s here, that know the stuff cold, and we don't believe it's possible to protect digital content. . . . [There is] this amazingly efficient distribution system for stolen property called the Internet—and no one's gonna shut down the Internet. And it only takes one stolen copy to be on the Internet. And the way we expressed it to them is: Pick one lock—open every door. It only takes one person to pick a lock. Worst case: Somebody just takes the analog outputs of their CD player and rerecords it—puts it on the Internet. You'll never stop that. So what you have to do is compete with it.[84]

Of course, when it was finally unveiled, Apple's iTunes Music Store did have copyright protection, doubtless at the insistence of the music industry. And, just as Jobs predicted, it has proven completely ineffective at preventing unauthorized copying.

Every notable DRM system ever created has been broken, usually within a few weeks of its introduction. There are strong theoretical reasons to think that developing an unbreakable DRM scheme is an impossible task.[85] After

years of vigorous effort to stamp them out, programs to circumvent every major DRM scheme—including Apple's FairPlay—are available from offshore websites. It is a battle the content owners and authorities cannot win.

Even if the authorities *could* remove every circumvention tool from the Internet, unscrupulous consumers would still have plenty of ways to get unprotected copies of copyrighted works. Music CDs are not encrypted, which means that anyone who owns a copy of a CD can "rip" it into an unprotected format like MP3 for unrestricted distribution. When J. K. Rowling released her latest blockbuster, *Harry Potter and the Halfblood Prince*, she chose not to release it in electronic format at all because of piracy concerns. That didn't stop people from scanning the book and converting it to electronic format. Illegal copies found their way onto peer-to-peer networks within 11 hours of the book's release.[86] No DRM technology could have prevented that.

Similarly, most copyrighted movies are available in VHS format or broadcast on TV. It is trivially easy to import such unprotected content into a computer. In other cases, pirates obtain copies of movies by smuggling a camcorder into movie theaters and recording the movie while it plays on the screen. Again, there's nothing DRM technology can do to prevent that.

In short, digital rights management is the Maginot Line of the war on piracy. The industry has gone to a great deal of effort to build elaborate defenses around protected files, but those defenses are completely useless as soon as just one person breaks through or goes around them, creates an unprotected file, and uploads it to a file-sharing network.

Voluntary Remedies

Fortunately, copyright holders have more effective, though imperfect, means to combat piracy. Some require no litigation at all. I've already mentioned the movie industry's "respect copyrights" campaign, which is designed to highlight the harms that movie piracy does to ordinary people in the movie industry. The recording industry also pays private firms to seed peer-to-peer networks with bogus versions of popular copyrighted songs, making it more difficult to find genuine copies of the files.[87]

Another powerful anti-piracy technique is to get software developers to voluntarily put anti-piracy "speedbumps" in their products. iTunes includes excellent examples of this approach. Consider the feature that allows iTunes users to share their music with others on their local network. It allows roommates, family members, or neighbors in a college dormitory to stream music between computers. But, crucially, the iTunes interface doesn't provide any means to copy music between machines, even if the music is not protected by the FairPlay DRM system. There is no technical reason for this limitation in the software. The developers of iTunes simply sought to do the right thing by voluntarily limiting the functionality of their software to encourage people to respect the law.

This isn't a foolproof piracy deterrent. The files aren't encrypted or otherwise copy protected, so any tech-savvy user could figure out how to access and copy the raw MP3 files. But, as we've seen, DRM schemes rarely stop determined infringers. On the other hand, such speed bumps are likely to be sufficient to deter the vast majority of casual copying by non-technically-savvy users, who are the vast majority of computer users. Most important, speed bumps do not require the force of law to be effective, and they have none of the harmful side effects documented in this paper.

Legal Remedies

Copyright holders also have powerful remedies in court against those not deterred by public appeals and technological speed bumps. As previously discussed, the Recording Industry Association of America began suing individual file sharers in 2003.[88] It filed its 10,000th lawsuit less than two years later.[89] Reports have indicated that most cases have been settled for between $3,000 and $4,000, which suggests

To protect free speech, we should be skeptical about any law that gives companies the opportunity to threaten those who criticize their products.

that the lawsuits could be largely self-financing.[90]

Such lawsuits may not be the most elegant solution. They are expensive and they clog an already-crowded court system. And in some cases they have raised civil liberties concerns, as Internet service providers are asked to turn over the personal details of thousands of individuals without proof of wrongdoing.[91] Congress might consider ways to streamline the process and strengthen the privacy of Internet users. Nevertheless, the lawsuits do appear to be having the desired effect: Users are on notice that the most egregious file sharers will be caught and prosecuted.

Lawsuits against individual file sharers are hardly the only legal tool at the disposal of the industry, however. As previously noted, the *Grokster* decision clearly established that companies that attempt to profit from illegal file sharing can be held responsible as contributory infringers.

Striking a Balance

Indeed, the principles underlying the *Grokster* decision are worth examining in some detail because they offer a sensible alternative to the technology-focused approach of the DMCA. In its decision, the Supreme Court declined to revisit the *Sony* precedent, which established that technologies with "substantial non-infringing uses" were not automatically liable for infringing activities with their products. Instead, the Court held that when there is clear evidence that a company intended to encourage copyright infringement among its users, the company is liable on the basis of its actions.

That puts the focus squarely where it belongs: on people rather than technologies. The high-tech landscape is too complex and dynamic for Congress or the courts to make rules about how companies may design technological devices. But human nature doesn't change very much. Courts are better equipped to judge the intentions of people than the technical merits of devices. If a future product is released and intellectual property owners charge that it is an illegal piracy device, the question the courts ought to ask is not, Does this device circumvent a DRM scheme? Rather, the appropriate question is, Do this company's actions undermine the right of copyright holders to profit from their creative efforts?

In *Sony*, the Supreme Court said that the law must "strike a balance between a copyright holder's legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce."[93] That balance can be struck effectively only if Congress articulates basic principles—as it did in the 1976 Copyright Act—and leaves the courts the flexibility to apply those principles to new technologies as they arise. When Congress opts instead to legislate about technological decisions, as it did in the DMCA, it leaves the courts no ability to strike the necessary balance as each new technology is released. And it creates a substantial risk that "substantially unrelated areas of commerce" will be caught in the crossfire. When used in concert with the anti-circumvention provisions of the DMCA, DRM schemes lock out unauthorized devices and restrict consumers' opportunities to use their legally purchased content in new ways.

Conclusion

In testimony before Congress in 1982, Jack Valenti warned that "the [VCR] is to the American film producer and the American public as the Boston strangler is to the woman home alone." Earlier in that same testimony, he said:

> The permission of the copyright owner is required for the use of [movies] in all markets. Those markets include theaters, cable, pay cable, pay television, prerecorded cassettes, network television, syndicated television, video discs. Every one of those markets is going to be competing for Mr. Eastwood's new

Digital rights management is the Maginot Line of the war on piracy.

film *Firefox*. They are going to license that film at a negotiated price.

> You simply cannot live in a marketplace where there is one unleashed animal in that marketplace, unlicensed. It would no longer be a marketplace; it would be a kind of a jungle, where this one unlicensed instrument is capable of devouring all that people had invested in and labored over and brought forth as a film or a television program, and, in short, laying waste to the orderly distribution of this product.[92]

Contrary to Valenti's predictions, the VCR turned out to be a great boon to the movie industry. Although some sales probably were lost to customers who chose to build libraries of movies recorded from TV, many consumers found the process too cumbersome and time-consuming and opted to purchase them instead. Meanwhile, within a few years, the "prerecorded cassette" market became a major revenue source in its own right. If this was Hollywood's Boston Strangler, every woman home alone should hope for a visit.

Yet, as Valenti's words reveal, the movie industry was fixated exclusively on the potential downside. Movie studios, like all large corporations, are conservative institutions. They have a strong interest in ensuring that the "orderly distribution" of their product continues undisturbed. If the marketplace becomes too dynamic and unpredictable, there is a real threat that some other company will find a way to sell the same products cheaper or more efficiently. When faced with a new industry innovation, they are especially likely to decide that the potential reward just is not worth the risk.

So it should concern us that the DMCA gives industry incumbents broad new powers to erect legal barriers to the introduction of new technologies. Given the industry's track record, there is little reason to think that incumbents will use those powers wisely or with restraint. More likely, they will view any consumer electronics product they do not fully control as a threat and refuse to allow such devices access to any of their content. They are likely to demand the removal of any feature that might threaten industry profits, no matter how much it might benefit consumers and even if it might hold out the possibility of new industry revenues.

Unfortunately, that take-no-prisoners approach to copyright protection will cause a lot of collateral damage. The "record" feature on a VCR really *does* have "substantial noninfringing uses," and they are not restricted to time shifting. In the *Sony* decision the Supreme Court noted that "representatives of professional baseball, football, basketball, and hockey testified that they had no objection to the recording of their televised events for home use." There is no good reason for the leagues to prevent sports fans from building a library of their favorite games, given that the leagues are unlikely to ever broadcast those events again. But that didn't stop the movie industry from trying to outlaw the "record" function on every VCR, regardless of the program being recorded.

By the same token, the consumer video marketplace of the future will be impoverished by the restrictions imposed by the OpenCable specifications. For example, a blogger commenting on the 2008 presidential race might want to include a video clip of a crucial exchange in one of the presidential debates. Or a sixth grader might want to include a short clip from the latest Harry Potter movie in a book report. The bandwidth and computing power to do such things are rapidly coming within the reach of the average consumer, and, under traditional copyright doctrine, such uses would likely be considered fair.

But the restrictions of OpenCable will likely make those uses impossible without violating the law. Converting copyrighted content into a format suitable for redistribution to the Internet is *verboten* by the OpenCable specification, regardless of whether doing so would constitute fair use.

The DMCA errs because it focuses on a technological means—circumvention—rather than a criminal end—piracy. People who circumvent DRM schemes to pirate content

The focus belongs on people rather than technologies.

should be punished, but people should be free to circumvent copy protection for purposes that are otherwise lawful. Sports fans should be free to record sports programs if the programs' owners do not object. Political junkies should be free to record public-interest programming that is in the public domain and redistribute it freely. Amateur movie buffs should be free to include short video clips in movie reviews, just as book reviewers include brief excerpts in book reviews. In short, consumers should not be punished if they circumvent copy protection for lawful purposes.

When the next breakthrough media device is invented, its inventor should not face a legal system in which the deck is stacked against him, as Streambox and DeCSS did. He should be free to focus on hiring the best programmers, designers, and marketers, rather than on shopping for a good law firm. If industry incumbents attempt to prevent his product from working with theirs, he should be allowed to circumvent the restrictions as Accolade did in the *Sega* case. And if the device has a "substantial non-infringing use" and is developed and marketed for such use, Congress and the courts should uphold its legality, even if it threatens the business model of an established industry.

The DMCA errs because it focuses on a technological means—circumvention—rather than a criminal end—piracy.

The Founding Fathers gave Congress the right to recognize copyrights in order to "promote the Progress of Science and the useful Arts." It hardly promotes progress to give a handful of companies the ability to tightly control how consumers use copyrighted content. Rather, progress is promoted in a technological marketplace of interoperable products, consumer choice, and fierce competition. The anti-circumvention provisions of the DMCA betray the constitutional vision. They impede rather than promote the progress of science and the useful arts.

Notes

1. There are exceptions. The biggest is the MP3.com case, discussed later in this section. Another is the case of ReplayTV, which was forced to remove the "30-second skip" feature from its Personal Video Recorder after its legal bills forced it into bankruptcy. Unfortunately, both cases were settled before they could be appealed.

2. This was first established in *Apple v. Franklin*, 714 F.2d 1240 (3d Cir. 1983), in which the court first held that a computer program is a "literary work and is protected from unauthorized copying" and that companies seeking to make "clones" of the Apple II computer could not simply copy Apple's software.

3. Phoenix's clean room technique and IBM's legal response are described in Russell Moy, "A Case against Software Patents," *Santa Clara Computer and High Technology Law Journal* 17 (2000): 72–73.

4. 977 F.2d 1510 (9th Cir. 1992).

5. 203 F.3d 596 (9th Cir. 2000).

6. 464 U.S. 417 (1984).

7. 180 F.3d 1072 (9th Cir. 1999).

8. Pub. L. No. 102-563 (codified at 17 U.S.C. § 1001 et seq.).

9. 180 F.3d at 1079.

10. Brad King, "Napster Faces Shutdown," *Wired News*, February 12, 2001, http://wired-vig.wired.com/news/politics/0,1283,41752,00.html.

11. 380 F.3d 1154 (9th Cir. 2004).

12. 125 S. Ct. 2764 (2005).

13. 92 F. Supp. 2d 349 (SDNY 2004).

14. Michelle Delio and Brad King, "MP3.Com Must Pay the Piper," *Wired News*, September 6, 2000, http://wired-vig.wired.com/news/business/0,1367,38613,00.html.

15. Amy Harmon, "Deal Settles Suit against MP3.com," *New York Times*, November 15, 2000.

16. As the Supreme Court put it in *Harper & Row v. Nation Enterprises*, 471 U.S. 539, 549 (1985), "Fair use was traditionally defined as 'a privilege in others than the owner of the copyright to use the copyrighted material in a reasonable manner without his consent.' The statutory formulation of the defense of fair use in the [1976] Copyright Act reflects the intent of Congress to codify the common-law doctrine."

17. 17 USCS § 107.

18. Lawrence Lessig. *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (New York: Penguin, 2004).

19. 336 F.3d 811 (9th Cir. 2003).

20. 510 U.S. 569.

21. Ibid. at 579.

22. U.S. Constitution, Art. 1, § 8.

23. Lynette Holloway, "Recording Industry to Sue Internet Music Swappers," *New York Times*, June 26, 2003.

24. Steve Knopper, "RIAA Will Keep On Suing," *Rolling Stone*, June 9, 2005, http://www.rollingstone.com/news/story/_/id/7380412.

25. The commercials can be downloaded from http://www.respectcopyrights.org/.

26. Encryption expert Bruce Schneier has an excellent description of this process in "The Futility of Digital Copy Prevention," *Crypto-gram newsletter*, May 15, 2001, http://www.schneier.com/crypto-gram-0105.html#3.

27. 17 USCS § 1201(a)(1)(A), (b)(1)(A).

28. Ibid. at (a)(2), (3).

29. Ibid. at § 1204.

30. Ibid. at 1201(a)(1)(B)-(C).

31. The other exemptions are for accessing the blacklists in Web filtering software, accessing programs that are protected by hardware "dongles" (hardware copy-protection devices that had their heyday in the 1980s after which they become inoperative and obsolete), and computer programs that require original, obsolete media to function. The full text of the librarian's determination is available at http://www.copyright.gov/fedreg/2003/68fr2011.pdf.

32. 17 USCS § 1201(d)(1).

33. Ibid. at § 1201(f).

34. Ibid. at § 1201(f)(3).

35. University of Minnesota law professor Dan Burk has suggested that these expanded rights be dubbed "paracopyright." Dan Burk, "Anticircumvention Misuse," 50 *UCLA Law Review* 1095 (2003). While the law was being considered, the House Commerce Committee version of the bill removed the anti-circumvention provision from Title 17 of the U.S. Code, the copyright title, because of its inconsistency with copyright. H. Rep. No. 105-551 at 24–25 (105th Cong., 2d sess.).

36. iTunes *does* allow users to "burn" a copy of their songs to CD and then "rip" the CD back to the user's hard drive in an unprotected format. It's not obvious what purpose is served by legally compelling users to waste a CD every time they want to transfer a song to a non-Apple product. And users who purchase videos from the iTunes store have no legal way to view them with non-Apple products.

37. 17 USCS § 1201(a)(1)(A), (a)(2)(A).

38. Stephen Manes, "Early Adopters of DVD Get Bragging Rights, and What Else?" *New York Times*, April 8, 1997.

39. In 2002 the Electronic Frontier Foundation proposed to the librarian of Congress that skipping DVD commercials be added to the list of circumvention activities exempted from the DMCA's prohibition on circumvention. The proposal, which describes the fast-forwarding problem in detail, is available from http://www.eff.org/IP/DMCA/20021218_EFFPKcomments.pdf.

40. See http://www.dvdcca.org/.

41. The acrimony between manufacturers and "diverters" is treated in depth in comments by Victory Wholesale Grocers (a company that specializes in product "diversion") submitted to a Federal Trade Commission Radio Frequency ID workshop, June 21, 2004. Victory quotes a document created by PepsiCo (a company that bitterly opposes "diverters"), which concedes, "Generally, in the absence of lawful contractual obligation to the contrary (e.g. a sampling program where there is an express provision stating that the product is sold at a discount only for distribution as part of such a program) resale of goods is not illegal." The comments are available at http://www.ftc.gov/os/comments/rfid-workshop/508920-0001.pdf.

42. For example, the Anti-Tampering Act of 1999, H.R. 2100 (106th Cong., 1st sess.), would have prohibited "altering or removing product identification codes from goods and packaging." Manufacturers' groups lobbied for the legislation, which would have made "diversion" much more difficult, but the bill never made it out of committee.

43. Amy Harmon,. "Movie Studios Seek to Stop DVD Copies," *New York Times*, July 18, 2000.

44. *Universal City Studios Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

45. Blue-Ray Disc Association,, "Blue-Ray Disc Association Adopts Comprehensive Content Management System," news release, August 9, 2005, http://www.blu-raydisc.com/assets/downloadablefile/050809-13034.pdf. For more information, see

Bill Rosenblatt, "Blu-ray Group Announces Content Protection Strategy," *DRM Watch*, August 11, 2005, http://www.drmwatch.com/drmtech/article.php/3526796.

46. Richard Shim and Jim Hu, "FAQ: CableCard? What's That?" *CNet News*, January 20, 2005, http://news.com.com/FAQ+CableCard+Whats+that/2100-1041_3-5542400.html

47. Stephen Speicher, "The Clicker: CableCARD and OpenCable," *Engadget*, April 14, 2005, http://www.engadget.com/entry/1234000343040219/.

48. The OpenCable specification is hundreds of pages long and spans multiple documents. The OpenCable System Security Specification is available at http://www.opencable.com/downloads/specs/OC-SP-SEC-I05-040831.pdf. The CableCARD Copy Protection System Interface Specification is available at http://www.opencable.com/downloads/specs/OC-SP-CCCP-IF-C01-050331.pdf.

49. Available at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516887764.

50. Richard Shim, "TiVo, Comcast Reach DVR Deal," *CNet News*, March 15, 2005, http://news.com.com/TiVo,+Comcast+reach+DVR+deal/2100-1041_3-5616961.html.

51. Saul Hansell, "Yahoo Plans to Connect Services with TiVo," *New York Times*, November 7, 2005.

52. Most Internet standards are described in documents known as requests for comments (RFCs), which are circulated among interested parties across the Internet prior to their adoption as formal standards. For example, the IP protocol is defined in RFC 791, http://www.faqs.org/rfcs/rfc791.html, and TCP is defined in RFC 793, http://www.faqs.org/rfcs/rfc793.html.

53. RFC 2161, http://www.faqs.org/rfcs/rfc2616.html.

54. The specification for HTML 4.01 is available at http://www.w3.org/TR/REC-html40/.

55. RFC 821, http://www.faqs.org/rfcs/rfc821.html.

56. This is, of course, a bit of a simplification. The leading Web browser, Internet Explorer, does not fully implement the HTML specification, and in an effort to ensure compatibility and stay competitive, other browsers have sometimes imitated Internet Explorer's rendering style. Nevertheless, a browser complying perfectly with HTTP and HTML would be able to display the vast majority of websites.

57. Real's streaming video product is the RealPlayer, available at http://www.real.com/player/. Microsoft's product is Windows Media Player, available at http://www.microsoft.com/windows/windowsmedia/. Apple's Quicktime is available at http://www.apple.com/quicktime/.

58. The exception is Google, which unveiled a new video player shortly before this paper went to press. Like those of the three incumbents, Google's format incorporates DRM functionality that renders it incompatible with other players on the market. Yahoo! and AOL are expected to roll out video-download services in early 2006 as well, although it is unclear whether these will license an existing format or introduce yet another (likely incompatible) one.

59. Sara Robinson, "RealNetworks Suit Defends Its Copyright on Audio Files," *New York Times*, December 30, 1999.

60. Monica Soto, "Deal Protects RealNetworks-Generated Files," *Seattle Times*, September 9, 2005.

61. *RealNetworks v. Streambox*, 2000 U.S. Dist. LEXIS 1889 (D. Wash. 2000).

62. 464 U.S. 417 (1984).

63. John Leyden, "Lexmark Unleashes DMCA on Toner Cartridge Rival," *Register*, January 10, 2003, http://www.theregister.co.uk/2003/01/10/lexmark_unleashes_dmca_on_toner/. The text of the complaint is available at http://www.eff.org/legal/cases/Lexmark_v_Static_Control/20030108_lexmark_v_static_control_components.pdf.

64. 387 F.3d 522 (6th Cir. 2004).

65. 292 F. Supp. 2d 1040, 1045 (D. Ill. 2003).

66. 381 F.3d 1178 (Fed. Cir. 2004).

67. 292 F. Supp. 2d 1040, 1045 (D. Ill. 2003).

68. 387 F.3d 522, 551 (6th Cir. 2004).

69. 387 F.3d at 530.

70. The iTunes terms of service are available at http://www.apple.com/support/itunes/legal/terms.html.

71. Jennifer 8. Lee, "U.S. Arrests Russian Cryptographer as Copyright Violator," *New York Times*, July 18, 2005.

72. Amy Harmon, "Adobe Opposes Prosecution in Hacking Case," *New York Times*, July 24, 2001.

73. Jennifer 8. Lee, "In Digital Copyright Case,

Programmer Can Go Home," *New York Times*, December 14, 2001.

74. Matt Richtel, "Russian Company Cleared of Illegal Software Sales," *New York Times*, December 18, 2002.

75. Thomas C. Greene, "SDMI Crack Team Scurries Away in Fear Again," *Register*, April 27, 2001, http://www.theregister.co.uk/2001/04/27/sdmi_crack_team_scurries_away/.

76. Thomas C. Greene, "SDMI Crack Team Launches Preemptive Suit," *Register*, June 7, 2001, http://www.theregister.co.uk/2001/06/07/sdmi_crack_team_launches_preemptive/.

77. Thomas C. Greene, "Felten Spills the SDMI Beans," *Register*, August 16, 2001, http://www.theregister.co.uk/2001/08/16/felten_spills_the_sdmi_beans/.

78. Declan McCullagh, "Security Warning Draws DMCA Threat," *CNet News*, July 30, 2002, http://news.com.com/2100-1023-947325.html.

79. Declan McCullagh, "HP Backs Down on Copyright Warning," *CNet News*, August 1, 2002, http://news.com.com/2100-1023-947745.html.

80. John Borland, "Court Blocks Security Conference Talk," *CNet News*, April 14, 2003, http://news.com.com/2100-1028-996836.html.

81. Hiawatha Bray, "Silence of a Code Cracker," *Boston Globe*, August 16, 2001.

82. Amy Harmon and Jennifer 8. Lee, "Arrest Raises Stakes in Battle over Copyright," *New York Times*, July 23, 2001.

83. Jack Valenti, "If You Cannot Protect What You Own, You Don't Own Anything! A Brief Report Concerning the Dark Underside of Internet Piracy as Well as the Possibility of a Cleansing Redemption to Benefit the American Consumer," Testimony before the Senate Committee on Commerce, Science and Transportation, February 28, 2002, http://commerce.senate.gov/hearings/022823 valenti.pdf.

84. Jeff Goodell, "Steve Jobs: The Rolling Stone Interview," *Rolling Stone*, December 3, 2003, http://www.rollingstone.com/news/story/_/id5939600?rnd=1131305689545.

85. The technical reasons why DRM systems are inherently insecure are beyond the scope of this paper, but security expert Bruce Schneier lays them out in a lecture titled "The Natural Laws of Digital Content." For a copy of the slides from a 2001 presentation, see http://www.ima.umn.edu/talks/workshops/2-12-16.2001/schneier/DigitalRights.pdf. See also http://crytome.org/futile-cp. htm.

86. Robert Andrews, "Pirates of the Potter-ian," *Wired News*, July 21, 2005, http://www.wired.com/news/digiwood/0,1412,68269,00.html?tw=wn_tophead_4.

87. "Record Labels Seed Song Sites with Fakes," *Houston Chronicle*, November 20, 2002.

88. Lynette Holloway, "Recording Industry to Sue Internet Music Swappers," *New York Times*, June 26, 2003.

89. The blog http://sharenomore.blogspot.com/ tallies RIAA lawsuits. On April 29, 2005, it noted that the RIAA had announced 725 new suits, bringing the total to 10,037. Judging from the RIAA's press releases since then, available at http://www.riaa.com/news/, the number had topped 13,000 by August 2005.

90. Steve Knopper, "RIAA Will Keep On Suing," *Rolling Stone*, June 9, 2005, http://www.rolling stone.com/news/story/_/id/7380412.

91. John Borland, "SBC Challenges RIAA over Subpoenas," *CNet News*, November 20, 2003, http://news.com.com/2100-1027_3-5110296.html.

92. Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Senate Committee on the Judiciary, April 12, 1982, available at http://cryptome.org/hrcw-hear. htm.

OTHER STUDIES IN THE POLICY ANALYSIS SERIES

563. **Against the New Paternalism: Internalities and the Economics of Self-Control** by Glen Whitman (February 22, 2006)

562. **KidSave: Real Problem, Wrong Solution** by Jagadeesh Gokhale and Michael Tanner (January 24, 2006)

561. **Economic Amnesia: The Case against Oil Price Controls and Windfall Profit Taxes** by Jerry Taylor and Peter Van Doren (January 12, 2006)

560. **Failed States and Flawed Logic: The Case against a Standing Nation-Building Office** by Justin Logan and Christopher Preble (January 11, 2006)

559. **A Desire Named Streetcar: How Federal Subsidies Encourage Wasteful Local Transit Systems** by Randal O'Toole (January 5, 2006)

558. **The Birth of the Property Rights Movement** by Steven J. Eagle (December 15, 2005)

557. **Trade Liberalization and Poverty Reduction in Sub-Saharan Africa** by Marian L. Tupy (December 6, 2005)

556. **Avoiding Medicare's Pharmaceutical Trap** by Doug Bandow (November 30, 2005)

555. **The Case against the Strategic Petroleum Reserve** by Jerry Taylor and Peter Van Doren (November 21, 2005)

554. **The Triumph of India's Market Reforms: The Record of the 1980s and 1990s** by Arvind Panagariya (November 7, 2005)

553. **U.S.-China Relations in the Wake of CNOOC** by James A. Dorn (November 2, 2005)

552. **Don't Resurrect the Law of the Sea Treaty** by Doug Bandow (October 13, 2005)

551. **Saving Money and Improving Education: How School Choice Can Help States Reduce Education Costs** by David Salisbury (October 4, 2005)

550. **The Personal Lockbox: A First Step on the Road to Social Security Reform** by Michael Tanner (September 13, 2005)

549. **Aging America's Achilles' Heel: Medicaid Long-Term Care** by Stephen A. Moses (September 1, 2005)

548. **Medicaid's Unseen Costs** by Michael F. Cannon (August 18, 2005)

547. **Uncompetitive Elections and the American Political System** by Patrick Basham and Dennis Polhill (June 30, 2005)

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001 or call toll free 1-800-767-1241 (8:30-4:30 eastern time). Fax (202) 842-3490 • www.cato.org

CATO INSTITUTE