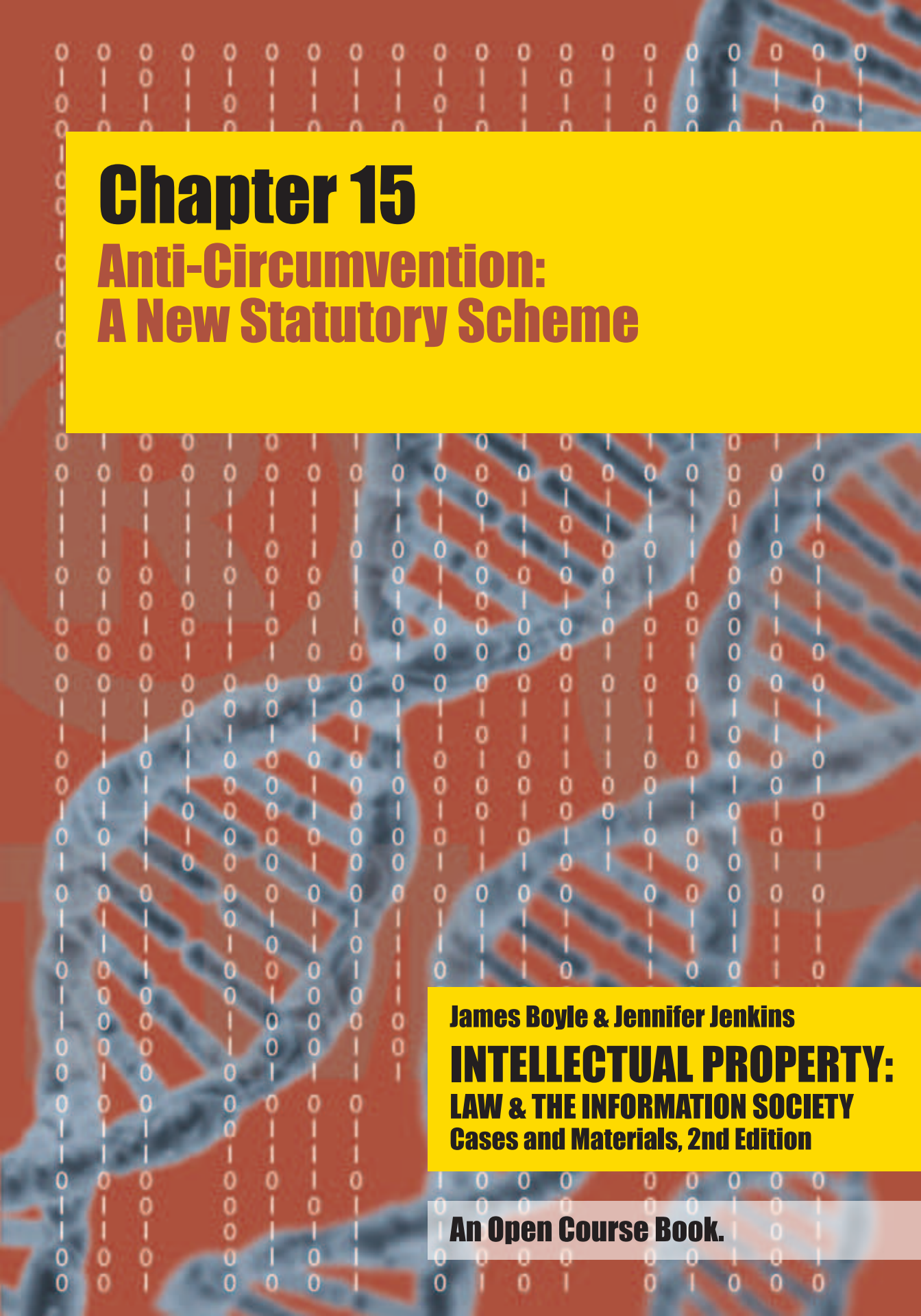

Chapter 15

Anti-Circumvention: A New Statutory Scheme

James Boyle & Jennifer Jenkins

INTELLECTUAL PROPERTY:
LAW & THE INFORMATION SOCIETY
Cases and Materials, 2nd Edition

An Open Course Book.

CHAPTER FIFTEEN
Anti-Circumvention: A New Statutory Scheme

§ 1201. Circumvention of copyright protection systems

(a) Violations Regarding Circumvention of Technological Measures

(1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter. . . .

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection —

(A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional Violations

(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection —

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

(c) Other Rights, Etc., Not Affected. —

(1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title. . . .

Introduction

The Digital Millennium Copyright Act ("DMCA") was passed in 1998 with the purported mission of "updating copyright law for the digital age." In the last chapter, you read about one of its key provisions—the safe harbors for service providers in section 512. As explained by the legislative history, these *limited* liability in order to "ensure[] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand." This chapter explores the countervailing provision of the DMCA that *expanded* potential liability. Quoting again from the legislative history: "Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy. [This legislation] provides this protection. . . ."

Specifically, Section 1201 of the DMCA added legal protection for "technological measures" employed by copyright owners either to prevent unauthorized access to their works ("access controls"), or to prevent copying, distribution, or other uses of their works that might infringe their exclusive rights ("rights controls"). You have probably encountered such technological measures—often referred to as "digital rights management" or "DRM." They might prevent you from "ripping" streaming audio or

video, modding video games, installing software on unauthorized devices, or printing and sharing eBooks beyond certain limitations. Which of these do you think are access controls, and which are rights controls?

Section 1201 can be difficult to parse; to assist you with understanding its structure, its basic provisions are summarized in the following chart.

§ 1201(a)(1)(A)—user prohibition	**§ 1201(a)(2)—trafficking ban**
←→	
Makes it illegal for a person to "circumvent a technological measure" that "effectively controls access" to a copyrighted work	Prohibits *trafficking* in tools that enable circumvention of *access* controls
[Old-school copyright infringement:	**§ 1201(b)(1)—additional violations**
←→	
User with lawful access infringes the copyright owner's § 106 rights of reproduction, distribution, making derivative works, public performance or display]	Prohibits *trafficking* in tools that enable circumvention of technological measures that protect the copyright owner's § 106 *rights*

Section 1201(a)(1)(A) (top left) prohibits users from circumventing technological measures that control access to copyrighted works. This focus on access was something new; before the DMCA, copyright law regulated *uses* that were reserved to rights holders by § 106, but did not regulate *access* to their works.

Section 1201 also added, in the right hand column, two provisions that go beyond the user, and prohibit anyone from "trafficking" in tools that defeat either access controls (§ 1201(a)(2)) or rights controls (§ 1201(b)(1)). For example, if the digital rights management (DRM) over your eBook prevents you from copying the book you just bought, a program that deactivates the DRM and allows you to store the book in an unprotected format would implicate § 1201(b)(1). Why? Because that DRM controlled *reproduction*, or copying, not access. By comparison, an "unlock" code that lets you watch a French Region 2 DVD on your American Region 1 DVD player would trigger § 1201(a)(2) because it gets around a measure that prevents *access* to the French film. (For those who haven't encountered "region coding," this is a technological measure used to geographically segment the movie market, so that customers in a given region can only watch movies officially released there.) These distinctions are not always clear-cut however; many technological measures both control access and protect § 106 rights. The tools that circumvent them could therefore violate both §§ 1201(a)(2) and (b)(1).

Moving into more contested territory: inevitably, many access controls will block both illegal and *legal* uses of a copyrighted work. DVD encryption might prevent you from making an illicit copy, but might also prevent you from excerpting a short clip for your class presentation within the bounds of "fair use." Can you be held liable for violating the DMCA if you decrypt the DVD in order to make a noninfringing use? What if someone else "traffics" in a tool—say, a decryption program—that allows you to make the noninfringing use; can that tool be enjoined? The cases in this chapter grapple with such questions, both in terms of statutory interpretation, and adherence with the Constitution. Does the language and structure of § 1201 flatly ban the circumvention of access controls, even when circumvention is necessary to engage in fair use? If so, can the DMCA be constitutional, when (as you read in *Eldred* and *Golan*) fair use is one of the two "traditional contours" that saves copyright law from running afoul of the First Amendment? Of course, the dangers might run the other way if a court were to allow certain circumvention tools in order to enable noninfringing uses: a decryption program that allows fair use could also be used to infringe copyright. Do we salvage user rights (such as fair use) at the expense of allowing some infringement? Or do we impose a

blanket prohibition on circumvention at the expense of impinging on user rights?

As you have seen in previous chapters, inserting computer code into the mix introduces additional complexities. First, in terms of potential *claims*, the fact that many everyday products contain copyrightable code leads to some interesting fact patterns. If I make a garage door opener that contains copyrighted code, and you develop a generic hand-held transmitter that—in order to open the garage door—has to bypass a technological control to access that code, have you violated the DMCA? Would you expect the DMCA to have anything to do with garage door openers? (This is a real case, and it's in your readings.)

By enjoining the distribution of certain types of computer code, does § 1201 run into First Amendment issues? Let's say the defendant's allegedly infringing *tool*, a DVD decryption program, enables circumvention. If the DMCA enjoins the distribution of that decryption program under its anti-trafficking rules, is it unconstitutionally suppressing speech? Is computer code "speech"? How would you frame the issue so that it was, or was not? (This case is also in the readings. Also, a heads' up to gamers: the final case in this chapter is about World of Warcraft.)

The exceptions in DMCA § 1201 are beyond the scope of this chapter, but a few things are worth mentioning here. Sections 1201(a)(1)(B)–(E) spell out an administrative rulemaking proceeding that takes place every three years and is supposed to enumerate certain "classes of works" for which circumvention (just the act of circumvention, not the tools enabling it) is allowed in order to make certain "noninfringing uses." In practice, these rulemakings have only yielded a handful of narrow exceptions. (They have never granted many of the exceptions you might expect, such as allowing owners of lawfully purchased DVDs to circumvent in order to make backup copies or watch them on DVD players from other regions.) Moreover, any exceptions expire after 3 years unless proponents make a new evidentiary showing that they're still warranted. For example, circumventing to "unlock" mobile phones in order to connect to a different wireless network was allowed in 2009 but then curtailed in 2012. In 2014, Congress stepped in to overrule that 2012 determination by passing the "Unlocking Consumer Choice and Wireless Competition Act," a new law that allows mobile phone unlocking on a permanent basis. (Yes, the 2014 Congress could not agree on much, but there was bipartisan support for reversing the DMCA rulemaking.) Sections 1201(d) through (j) of the DMCA provide other limited exceptions for libraries, archives, and educational institutions; law enforcement; reverse engineering; encryption research; protecting minors; disabling cookies; and security testing. They vary in scope, and some are extremely circumscribed (read the text of § 1201(d) for an example of this).

James Boyle, The Public Domain

Please read The Public Domain pp. 83–89

Imagine that a bustling group of colonists has just moved into a new area, a huge,

unexplored plain. (Again, assume the native inhabitants have conveniently disappeared.) Some of the colonists want to farm just as they always did in the old country. "Good fences make good neighbors" is their motto. Others, inspired by the wide-open spaces around them, declare that this new land needs new ways. They want to let their cattle roam as they will; their slogan is "Protect the open range." In practice, the eventual result is a mixture of the two regimes. Fields under cultivation can be walled off but there is a right of passage through the farmers' lands for all who want it, so long as no damage is done. This means travelers do not need to make costly and inefficient detours around each farm. In the long run, these "public roads" actually increase the value of the private property through which they pass. They also let the ranchers move their cattle around from one area of pasture to another. The ranchers become strong proponents of "public, open highways" (though some people muse darkly that they do very well out of that rule). Still, most people want open highways; the system seems to work pretty well, in fact. . . .

Read the rest

1.) Anti-Circumvention, Fair Use, and the First Amendment

Universal City Studios, Inc. v. Corley

273 F.3d 429 (2d Cir. 2001)

JON O. NEWMAN, Circuit Judge.

When the Framers of the First Amendment prohibited Congress from making any law "abridging the freedom of speech," they were not thinking about computers, computer programs, or the Internet. But neither were they thinking about radio, television, or movies. Just as the inventions at the beginning and middle of the 20th century presented new First Amendment issues, so does the cyber revolution at the end of that century. This appeal raises significant First Amendment issues concerning one aspect of computer technology—encryption to protect materials in digital form from unauthorized access. The appeal challenges the constitutionality of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 *et seq.* and the validity of an injunction entered to enforce the DMCA.

Defendant-Appellant Eric C. Corley and his company, 2600 Enterprises, Inc., (appeal from the amended final judgment of the United States District Court for the Southern District of New York enjoining them from various actions concerning a decryption program known as "DeCSS." The injunction primarily bars the Appellants from posting DeCSS on their web site and from knowingly linking their web site to any other web site on which DeCSS is posted. We affirm.

Introduction

This appeal concerns the anti-trafficking provisions of the DMCA, which

Congress enacted in 1998 to strengthen copyright protection in the digital age. Fearful that the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material, Congress sought to combat copyright piracy in its earlier stages, before the work was even copied. The DMCA therefore backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections. In so doing, Congress targeted not only those pirates who would *circumvent* these digital walls (the "anti-circumvention provisions," contained in 17 U.S.C. § 1201(a)(1)), but also anyone who would *traffic* in a technology primarily designed to circumvent a digital wall (the "anti-trafficking provisions," contained in 17 U.S.C. §§ 1201(a)(2), (b)(1)).

Corley publishes a print magazine and maintains an affiliated web site geared towards "hackers," a digital-era term often applied to those interested in techniques for circumventing protections of computers and computer data from unauthorized access. The so-called hacker community includes serious computer-science scholars conducting research on protection techniques, computer buffs intrigued by the challenge of trying to circumvent access-limiting devices or perhaps hoping to promote security by exposing flaws in protection techniques, mischief-makers interested in disrupting computer operations, and thieves, including copyright infringers who want to acquire copyrighted material (for personal use or resale) without paying for it.

In November 1999, Corley posted a copy of the decryption computer program "DeCSS" on his web site, http://www.2600.com.[2] DeCSS is designed to circumvent "CSS," the encryption technology that motion picture studios place on DVDs to prevent the unauthorized viewing and copying of motion pictures. Corley also posted on his web site links to other web sites where DeCSS could be found.

Plaintiffs-Appellees are eight motion picture studios that brought an action . . . seeking injunctive relief against Corley under the DMCA. . . . [T]he District Court entered a permanent injunction barring Corley from posting DeCSS on his web site or from knowingly linking via a hyperlink to any other web site containing DeCSS. The District Court rejected Corley's constitutional attacks on the statute and the injunction.

Corley renews his constitutional challenges on appeal. Specifically, he argues primarily that: (1) the DMCA oversteps limits in the Copyright Clause on the duration of copyright protection; (2) the DMCA as applied to his dissemination of DeCSS violates the First Amendment because computer code is "speech" entitled to full First Amendment protection and the DMCA fails to survive the exacting scrutiny accorded statutes that regulate "speech"; and (3) the DMCA violates the First Amendment and the Copyright Clause by unduly obstructing the "fair use" of copyrighted materials. Corley also argues that the statute is susceptible to, and should therefore be given, a narrow interpretation that avoids alleged constitutional objections.

Background

For decades, motion picture studios have made movies available for viewing at home in what is called "analog" format. Movies in this format are placed on videotapes,

[2] "2600" has special significance to the hacker community. It is the hertz frequency of a signal that some hackers formerly used to explore the entire telephone system from "operator mode," which was triggered by the transmission of a 2600 hertz tone across a telephone line, or to place telephone calls without incurring long-distance toll charges. One such user reportedly discovered that the sound of a toy whistle from a box of Cap'n Crunch cereal matched the telephone company's 2600 hertz tone perfectly.

which can be played on a video cassette recorder ("VCR"). In the early 1990s, the studios began to consider the possibility of distributing movies in digital form as well. Movies in digital form are placed on disks, known as DVDs, which can be played on a DVD player (either a stand-alone device or a component of a computer). DVDs offer advantages over analog tapes, such as improved visual and audio quality, larger data capacity, and greater durability. However, the improved quality of a movie in a digital format brings with it the risk that a virtually perfect copy, *i.e.,* one that will not lose perceptible quality in the copying process, can be readily made at the click of a computer control and instantly distributed to countless recipients throughout the world over the Internet. This case arises out of the movie industry's efforts to respond to this risk by invoking the anti-trafficking provisions of the DMCA.

I. CSS

The movie studios were reluctant to release movies in digital form until they were confident they had in place adequate safeguards against piracy of their copyrighted movies. The studios took several steps to minimize the piracy threat. First, they settled on the DVD as the standard digital medium for home distribution of movies. The studios then sought an encryption scheme to protect movies on DVDs. They enlisted the help of members of the consumer electronics and computer industries, who in mid-1996 developed the Content Scramble System ("CSS"). CSS is an encryption scheme that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. The algorithm is a type of mathematical formula for transforming the contents of the movie file into gibberish; the "keys" are in actuality strings of 0's and 1's that serve as values for the mathematical formula. Decryption in the case of CSS requires a set of "player keys" contained in compliant DVD players, as well as an understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the contents of a DVD. With the player keys and the algorithm, a DVD player can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content of the DVD.

The studios developed a licensing scheme for distributing the technology to manufacturers of DVD players. Player keys and other information necessary to the CSS scheme were given to manufacturers of DVD players for an administrative fee. In exchange for the licenses, manufacturers were obliged to keep the player keys confidential. Manufacturers were also required in the licensing agreement to prevent the transmission of "CSS data" (a term undefined in the licensing agreement) from a DVD drive to any "internal recording device," including, presumably, a computer hard drive.

With encryption technology and licensing agreements in hand, the studios began releasing movies on DVDs in 1997, and DVDs quickly gained in popularity, becoming a significant source of studio revenue. In 1998, the studios secured added protection against DVD piracy when Congress passed the DMCA, which prohibits the development or use of technology designed to circumvent a technological protection measure, such as CSS. The pertinent provisions of the DMCA are examined in greater detail below.

II. DeCSS

In September 1999, Jon Johansen, a Norwegian teenager, collaborating with two unidentified individuals he met on the Internet, reverse-engineered a licensed DVD player designed to operate on the Microsoft operating system, and culled from it the player keys and other information necessary to decrypt CSS. The record suggests that Johansen was trying to develop a DVD player operable on Linux, an alternative operating system that did not support any licensed DVD players at that time. In order to accomplish

this task, Johansen wrote a decryption program executable on Microsoft's operating system. That program was called, appropriately enough, "DeCSS."

If a user runs the DeCSS program . . . with a DVD in the computer's disk drive, DeCSS will decrypt the DVD's CSS protection, allowing the user to copy the DVD's files and place the copy on the user's hard drive. The result is a very large computer file that can be played on a non-CSS-compliant player and copied, manipulated, and transferred just like any other computer file. DeCSS comes complete with a fairly user-friendly interface that helps the user select from among the DVD's files and assign the decrypted file a location on the user's hard drive. The quality of the resulting decrypted movie is "virtually identical" to that of the encrypted movie on the DVD. And the file produced by DeCSS, while large, can be compressed to a manageable size by a compression software called "DivX," available at no cost on the Internet. This compressed file can be copied onto a DVD, or transferred over the Internet (with some patience).

Johansen posted the executable object code, but not the source code, for DeCSS on his web site. . . . Within months of its appearance in executable form on Johansen's web site, DeCSS was widely available on the Internet, in both object code and various forms of source code.

In November 1999, Corley wrote and placed on his web site, 2600.com, an article about the DeCSS phenomenon. His web site is an auxiliary to the print magazine, *2600: The Hacker Quarterly*, which Corley has been publishing since 1984. As the name suggests, the magazine is designed for "hackers," as is the web site. While the magazine and the web site cover some issues of general interest to computer users—such as threats to online privacy—the focus of the publications is on the vulnerability of computer security systems, and more specifically, how to exploit that vulnerability in order to circumvent the security systems. Representative articles explain how to steal an Internet domain name and how to break into the computer systems at Federal Express.

Corley's article about DeCSS detailed how CSS was cracked, and described the movie industry's efforts to shut down web sites posting DeCSS. It also explained that DeCSS could be used to copy DVDs. At the end of the article, the Defendants posted copies of the object and source code of DeCSS. In Corley's words, he added the code to the story because "in a journalistic world, . . . [y]ou have to show your evidence . . . and particularly in the magazine that I work for, people want to see specifically what it is that we are referring to," including "what evidence . . . we have" that there is in fact technology that circumvents CSS. Writing about DeCSS without including the DeCSS code would have been, to Corley, "analogous to printing a story about a picture and not printing the picture." Corley also added to the article links that he explained would take the reader to other web sites where DeCSS could be found.

2600.com was only one of hundreds of web sites that began posting DeCSS near the end of 1999. The movie industry tried to stem the tide by sending cease-and-desist letters to many of these sites. These efforts met with only partial success; a number of sites refused to remove DeCSS. In January 2000, the studios filed this lawsuit.

III. The DMCA

The DMCA was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty ("WIPO Treaty"), which requires contracting parties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law." Even before the treaty, Congress had been devoting attention to the

problems faced by copyright enforcement in the digital age. Hearings on the topic have spanned several years. This legislative effort resulted in the DMCA.

The Act contains three provisions targeted at the circumvention of technological protections. The first is subsection 1201(a)(1)(A), the anti-circumvention provision. This provision prohibits a person from "circumvent[ing] a technological measure that effectively controls access to a work protected under [Title 17, governing copyright]." The Librarian of Congress is required to promulgate regulations every three years exempting from this subsection individuals who would otherwise be "adversely affected" in "their ability to make noninfringing uses." 17 U.S.C. §§ 1201(a)(1)(B)–(E).

The second and third provisions are subsections 1201(a)(2) and 1201(b)(1), the "anti-trafficking provisions." Subsection 1201(a)(2), the provision at issue in this case, provides:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

To "circumvent a technological measure" is defined, in pertinent part, as "to descramble a scrambled work . . . or otherwise to . . . bypass . . . a technological measure, without the authority of the copyright owner." § 1201(a)(3)(A).

Subsection 1201(b)(1) is similar to subsection 1201(a)(2), except that subsection 1201(a)(2) covers those who traffic in technology that can circumvent "a technological measure *that effectively controls access* to a work protected under" Title 17, whereas subsection 1201(b)(1) covers those who traffic in technology that can circumvent "protection afforded by a technological measure *that effectively protects a right of a copyright owner* under" Title 17. §§ 1201(a)(2), (b)(1) (emphases added). In other words, although both subsections prohibit trafficking in a circumvention technology, the focus of subsection 1201(a)(2) is circumvention of technologies designed to *prevent access* to a work, and the focus of subsection 1201(b)(1) is circumvention of technologies designed to *permit access* to a work but *prevent copying* of the work or some other act that infringes a copyright. Subsection 1201(a)(1) differs from both of these anti-trafficking subsections in that it targets the use of a circumvention technology, not the trafficking in such a technology.

The DMCA contains exceptions for schools and libraries that want to use circumvention technologies to determine whether to purchase a copyrighted product, 17 U.S.C. § 1201(d); individuals using circumvention technology "for the sole purpose" of trying to achieve "interoperability" of computer programs through reverse-engineering, § 1201(f); encryption research aimed at identifying flaws in encryption technology, if the research is conducted to advance the state of knowledge in the field, § 1201(g); and several other exceptions not relevant here.

The DMCA creates civil remedies, § 1203, and criminal sanctions, § 1204. It specifically authorizes a court to "grant temporary and permanent injunctions on such

terms as it deems reasonable to prevent or restrain a violation." § 1203(b)(1).

IV. Procedural History

. . . After a trial on the merits, the [District] Court issued a comprehensive opinion, and granted a permanent injunction.

The Court explained that the Defendants' posting of DeCSS on their web site clearly falls within section 1201(a)(2)(A) of the DMCA, rejecting as spurious their claim that CSS is not a technological measure that "effectively controls access to a work" because it was so easily penetrated by Johansen, and as irrelevant their contention that DeCSS was designed to create a Linux-platform DVD player. The Court also held that the Defendants cannot avail themselves of any of the DMCA's exceptions, and that the alleged importance of DeCSS to certain fair uses of encrypted copyrighted material was immaterial to their statutory liability. The Court went on to hold that when the Defendants "proclaimed on their own site that DeCSS could be had by clicking on the hyperlinks" on their site, they were trafficking in DeCSS, and therefore liable for their linking as well as their posting.

Turning to the Defendants' numerous constitutional arguments, the Court first held that computer code like DeCSS is "speech" that is "protected" (in the sense of "covered") by the First Amendment, but that because the DMCA is targeting the "functional" aspect of that speech, it is "content neutral," and the intermediate scrutiny of *United States v. O'Brien* (1968), applies. The Court concluded that the DMCA survives this scrutiny, and also rejected prior restraint, overbreadth, and vagueness challenges. . . .

Discussion

I. Narrow Construction to Avoid Constitutional Doubt

The Appellants first argue that, because their constitutional arguments are at least substantial, we should interpret the statute narrowly so as to avoid constitutional problems. They identify three different instances of alleged ambiguity in the statute that they claim provide an opportunity for such a narrow interpretation.

First, they contend that subsection 1201(c)(1), which provides that "[n]othing in this section shall affect rights, remedies, limitations or defenses to copyright infringement, including fair use, under this title," can be read to allow the circumvention of encryption technology protecting copyrighted material when the material will be put to "fair uses" exempt from copyright liability. We disagree that subsection 1201(c)(1) permits such a reading. Instead, it simply clarifies that the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the *use* of those materials after circumvention has occurred. Subsection 1201(c)(1) ensures that the DMCA is not read to prohibit the "fair use" of information just because that information was obtained in a manner made illegal by the DMCA. The Appellants' much more expansive interpretation of subsection 1201(c)(1) is not only outside the range of plausible readings of the provision, but is also clearly refuted by the statute's legislative history.[13]

---

[13] The legislative history of the enacted bill makes quite clear that Congress intended to adopt a "balanced" approach to accommodating both piracy and fair use concerns, eschewing the quick fix of simply exempting from the statute all circumventions for fair use. It sought to achieve this goal principally through the use of what it called a "fail-safe" provision in the statute, authorizing the Librarian of Congress to exempt certain users from the anti-circumvention provision when it becomes evident that in practice, the statute is adversely affecting certain kinds of fair use. Congress also sought to implement a balanced approach through statutory provisions that leave limited areas of breathing space for fair use. A good example is subsection 1201(d),

Second, the Appellants urge a narrow construction of the DMCA because of subsection 1201(c)(4), which provides that "[n]othing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products." This language is clearly precatory: Congress could not "diminish" constitutional rights of free speech even if it wished to, and the fact that Congress also expressed a reluctance to "enlarge" those rights cuts against the Appellants' effort to infer a narrowing construction of the Act from this provision.

Third, the Appellants argue that an individual who buys a DVD has the "authority of the copyright owner" to view the DVD, and therefore is exempted from the DMCA pursuant to subsection 1201(a)(3)(A) when the buyer circumvents an encryption technology in order to view the DVD on a competing platform (such as Linux). The basic flaw in this argument is that it misreads subsection 1201(a)(3)(A). That provision exempts from liability those who would "decrypt" an encrypted DVD with the authority of a copyright owner, not those who would "view" a DVD with the authority of a copyright owner. In any event, the Defendants offered no evidence that the Plaintiffs have either explicitly or implicitly authorized DVD buyers to circumvent encryption technology to support use on multiple platforms.[15]

We conclude that the anti-trafficking and anti-circumvention provisions of the DMCA are not susceptible to the narrow interpretations urged by the Appellants. We therefore proceed to consider the Appellants' constitutional claims.

II. Constitutional Challenge Based on the Copyright Clause

In a footnote to their brief, the Appellants appear to contend that the DMCA, as construed by the District Court, exceeds the constitutional authority of Congress to grant authors copyrights for a "limited time," U.S. Const. art. I, § 8, cl. 8, because it "empower[s] copyright owners to effectively secure perpetual protection by mixing public domain works with copyrighted materials, then locking both up with technological protection measures." This argument is elaborated in the *amici curiae* brief filed by Prof. Julie E. Cohen on behalf of herself and 45 other intellectual property law professors. For two reasons, the argument provides no basis for disturbing the judgment of the District Court.

First, we have repeatedly ruled that arguments presented to us only in a footnote are not entitled to appellate consideration. Although an *amicus* brief can be helpful in elaborating issues properly presented by the parties, it is normally not a method for injecting new issues into an appeal, at least in cases where the parties are competently represented by counsel.

Second, to whatever extent the argument might have merit at some future time in a case with a properly developed record, the argument is entirely premature and speculative at this time on this record. There is not even a claim, much less evidence, that any Plaintiff has sought to prevent copying of public domain works, or that the injunction prevents the Defendants from copying such works. As Judge Kaplan noted,

---

which allows a library or educational institution to circumvent a digital wall in order to determine whether it wishes legitimately to obtain the material behind the wall. It would be strange for Congress to open small, carefully limited windows for circumvention to permit fair use in subsection 1201(d) if it then meant to exempt in subsection 1201(c)(1) *any* circumvention necessary for fair use.

[15] Even if the Defendants had been able to offer such evidence, and even if they could have demonstrated that DeCSS was "primarily designed . . . for the purpose of" playing DVDs on multiple platforms (and therefore not for the purpose of "circumventing a technological measure"), a proposition questioned by Judge Kaplan, the Defendants would defeat liability only under subsection 1201(a)(2)(A). They would still be vulnerable to liability under subsection 1201(a)(2)(C), because they "marketed" DeCSS for the copying of DVDs, not just for the playing of DVDs on multiple platforms.

the possibility that encryption would preclude access to public domain works "does not yet appear to be a problem, although it may emerge as one in the future."

III. Constitutional Challenges Based on the First Amendment

A. Applicable Principles

Last year, in one of our Court's first forays into First Amendment law in the digital age, we took an "evolutionary" approach to the task of tailoring familiar constitutional rules to novel technological circumstances, favoring "narrow" holdings that would permit the law to mature on a "case-by-case" basis. In that spirit, we proceed, with appropriate caution, to consider the Appellants' First Amendment challenges by analyzing a series of preliminary issues the resolution of which provides a basis for adjudicating the specific objections to the DMCA and its application to DeCSS. These issues, which we consider only to the extent necessary to resolve the pending appeal, are whether computer code is speech, whether computer programs are speech, the scope of First Amendment protection for computer code, and the scope of First Amendment protection for decryption code. . . .

1. Code as Speech

Communication does not lose constitutional protection as "speech" simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in "code," *i.e.,* symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment. If someone chose to write a novel entirely in computer object code by using strings of 1's and 0's for each letter of each word, the resulting work would be no different for constitutional purposes than if it had been written in English. The "object code" version would be incomprehensible to readers outside the programming community (and tedious to read even for most within the community), but it would be no more incomprehensible than a work written in Sanskrit for those unversed in that language. The undisputed evidence reveals that even pure object code can be, and often is, read and understood by experienced programmers. And source code (in any of its various levels of complexity) can be read by many more. Ultimately, however, the ease with which a work is comprehended is irrelevant to the constitutional inquiry. If computer code is distinguishable from conventional speech for First Amendment purposes, it is not because it is written in an obscure language.

2. Computer Programs as Speech

Of course, computer code is not likely to be the language in which a work of literature is written. Instead, it is primarily the language for programs executable by a computer. These programs are essentially instructions to a computer. In general, programs may give instructions either to perform a task or series of tasks when initiated by a single (or double) click of a mouse or, once a program is operational ("launched"), to manipulate data that the user enters into the computer. Whether computer code that gives a computer instructions is "speech" within the meaning of the First Amendment requires consideration of the scope of the Constitution's protection of speech.

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech. . . ." U.S. Const. amend. I. "Speech" is an elusive term, and judges and scholars have debated its bounds for two centuries. Some would confine First Amendment protection to political speech. Others would extend it further to artistic expression.

Whatever might be the merits of these and other approaches, the law has not been so limited. Even dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded First Amendment protection.

Thus, for example, courts have subjected to First Amendment scrutiny restrictions

on the dissemination of technical scientific information and scientific research, and attempts to regulate the publication of instructions, *see, e.g., United States v. Raymond* (7th Cir. 2000) (First Amendment does not protect instructions for violating the tax laws); *Herceg v. Hustler Magazine, Inc.* (5th Cir. 1987) (First Amendment protects instructions for engaging in a dangerous sex act); *United States v. Featherston* (5th Cir. 1972) (First Amendment does not protect instructions for building an explosive device).

Computer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer. A recipe is no less "speech" because it calls for the use of an oven, and a musical score is no less "speech" because it specifies performance on an electric guitar. Arguably distinguishing computer programs from conventional language instructions is the fact that programs are executable on a computer. But the fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions "speech" for purposes of the First Amendment. The information conveyed by most "instructions" is how to perform a task.

Instructions such as computer code, which are intended to be executable by a computer, will often convey information capable of comprehension and assessment by a human being. A programmer reading a program learns information about instructing a computer, and might use this information to improve personal programming skills and perhaps the craft of programming. Moreover, programmers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes. Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars, just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression. Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both). . . .

For all of these reasons, we join the other courts that have concluded that computer code, and computer programs constructed from code can merit First Amendment protection, although the scope of such protection remains to be determined.

3. The Scope of First Amendment Protection for Computer Code

Having concluded that computer code conveying information is "speech" within the meaning of the First Amendment, we next consider, to a limited extent, the scope of the protection that code enjoys. As the District Court recognized, the scope of protection for speech generally depends on whether the restriction is imposed because of the content of the speech. Content-based restrictions are permissible only if they serve compelling state interests and do so by the least restrictive means available. A content-neutral restriction is permissible if it serves a substantial governmental interest, the interest is unrelated to the suppression of free expression, and the regulation is narrowly tailored, which "in this context requires . . . that the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" *Turner Broadcasting System, Inc. v. FCC* (1994).

"[G]overnment regulation of expressive activity is 'content neutral' if it is justified without reference to the content of regulated speech." *Hill v. Colorado* (2000). "The government's purpose is the controlling consideration. A regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others." *Ward v. Rock Against Racism* (1989). The Supreme Court's approach to determining content-neutrality appears to be applicable

whether what is regulated is expression, conduct, or any "activity" that can be said to combine speech and non-speech elements.

To determine whether regulation of computer code is content-neutral, the initial inquiry must be whether the regulated activity is "sufficiently imbued with elements of communication to fall within the scope of the First . . . Amendment[]." . . . Once a speech component is identified, the inquiry then proceeds to whether the regulation is "justified without reference to the content of regulated speech." *Hill*.

The Appellants vigorously reject the idea that computer code can be regulated according to any different standard than that applicable to pure speech, *i.e.,* speech that lacks a nonspeech component. Although recognizing that code is a series of instructions to a computer, they argue that code is no different, for First Amendment purposes, than blueprints that instruct an engineer or recipes that instruct a cook. We disagree. Unlike a blueprint or a recipe, which cannot yield any functional result without human comprehension of its content, human decision-making, and human action, computer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the Internet. The only human action required to achieve these results can be as limited and instantaneous as a single click of a mouse. These realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, *i.e.,* functional and expressive elements.

We recognize, as did Judge Kaplan, that the functional capability of computer code cannot yield a result until a human being decides to insert the disk containing the code into a computer and causes it to perform its function (or programs a computer to cause the code to perform its function). Nevertheless, this momentary intercession of human action does not diminish the nonspeech component of code, nor render code entirely speech, like a blueprint or a recipe. Judge Kaplan, in a passage that merits extensive quotation, cogently explained why this is especially so with respect to decryption code:

> [T]he focus on functionality in order to determine the level of scrutiny is not an inevitable consequence of the speech-conduct distinction. Conduct has immediate effects on the environment. Computer code, on the other hand, no matter how functional, causes a computer to perform the intended operations only if someone uses the code to do so. Hence, one commentator, in a thoughtful article, has maintained that functionality is really "a proxy for effects or harm" and that its adoption as a determinant of the level of scrutiny slides over questions of causation that intervene between the dissemination of a computer program and any harm caused by its use. The characterization of functionality as a proxy for the consequences of use is accurate. But the assumption that the chain of causation is too attenuated to justify the use of functionality to determine the level of scrutiny, at least in this context, is not. Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used. . . . There

> was a time when copyright infringement could be dealt with quite adequately by focusing on the infringing act. If someone wished to make and sell high quality but unauthorized copies of a copyrighted book, for example, the infringer needed a printing press. The copyright holder, once aware of the appearance of infringing copies, usually was able to trace the copies up the chain of distribution, find and prosecute the infringer, and shut off the infringement at the source. In principle, the digital world is very different. Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD. The process potentially is exponential rather than linear. . . . These considerations drastically alter consideration of the causal link between dissemination of computer programs such as this and their illicit use. Causation in the law ultimately involves practical policy judgments. Here, dissemination itself carries very substantial risk of imminent harm because the mechanism is so unusual by which dissemination of means of circumventing access controls to copyrighted works threatens to produce virtually unstoppable infringement of copyright. In consequence, the causal link between the dissemination of circumvention computer programs and their improper use is more than sufficiently close to warrant selection of a level of constitutional scrutiny based on the programs' functionality.

The functionality of computer code properly affects the scope of its First Amendment protection.

4. The Scope of First Amendment Protection for Decryption Code

In considering the scope of First Amendment protection for a decryption program like DeCSS, we must recognize that the essential purpose of encryption code is to prevent unauthorized access. Owners of all property rights are entitled to prohibit access to their property by unauthorized persons. Homeowners can install locks on the doors of their houses. Custodians of valuables can place them in safes. Stores can attach to products security devices that will activate alarms if the products are taken away without purchase. These and similar security devices can be circumvented. Burglars can use skeleton keys to open door locks. Thieves can obtain the combinations to safes. Product security devices can be neutralized.

Our case concerns a security device, CSS computer code, that prevents access by unauthorized persons to DVD movies. The CSS code is embedded in the DVD movie. Access to the movie cannot be obtained unless a person has a device, a licensed DVD player, equipped with computer code capable of decrypting the CSS encryption code. In its basic function, CSS is like a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products.

DeCSS is computer code that can decrypt CSS. In its basic function, it is like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize the security device attached to a store's products.[27] DeCSS enables anyone to gain access to a DVD movie without using a DVD player.

The initial use of DeCSS to gain access to a DVD movie creates no loss to movie

[27] More dramatically, the Government calls DeCSS "a digital crowbar."

producers because the initial user must purchase the DVD. However, once the DVD is purchased, DeCSS enables the initial user to copy the movie in digital form and transmit it instantly in virtually limitless quantity, thereby depriving the movie producer of sales. The advent of the Internet creates the potential for instantaneous worldwide distribution of the copied material.

At first glance, one might think that Congress has as much authority to regulate the distribution of computer code to decrypt DVD movies as it has to regulate distribution of skeleton keys, combinations to safes, or devices to neutralize store product security devices. However, despite the evident legitimacy of protection against unauthorized access to DVD movies, just like any other property, regulation of decryption code like DeCSS is challenged in this case because DeCSS differs from a skeleton key in one important respect: it not only is capable of performing the function of unlocking the encrypted DVD movie, it also is a form of communication, albeit written in a language not understood by the general public. As a communication, the DeCSS code has a claim to being "speech," and as "speech," it has a claim to being protected by the First Amendment. But just as the realities of what any computer code can accomplish must inform the scope of its constitutional protection, so the capacity of a decryption program like DeCSS to accomplish unauthorized—indeed, unlawful—access to materials in which the Plaintiffs have intellectual property rights must inform and limit the scope of its First Amendment protection. . . .

B. First Amendment Challenge

The District Court's injunction applies the DMCA to the Defendants by imposing two types of prohibition, both grounded on the anti-trafficking provisions of the DMCA. The first prohibits posting DeCSS or any other technology for circumventing CSS on any Internet web site. The second prohibits knowingly linking any Internet web site to any other web site containing DeCSS. . . .

1. Posting

. . .

As a content-neutral regulation with an incidental effect on a speech component, the regulation must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest. The Government's interest in preventing unauthorized access to encrypted copyrighted material is unquestionably substantial, and the regulation of DeCSS by the posting prohibition plainly serves that interest. Moreover, that interest is unrelated to the suppression of free expression. The injunction regulates the posting of DeCSS, regardless of whether DeCSS code contains any information comprehensible by human beings that would qualify as speech. Whether the incidental regulation on speech burdens substantially more speech than is necessary to further the interest in preventing unauthorized access to copyrighted materials requires some elaboration.

Posting DeCSS on the Appellants' web site makes it instantly available at the click of a mouse to any person in the world with access to the Internet, and such person can then instantly transmit DeCSS to anyone else with Internet access. Although the prohibition on posting prevents the Appellants from conveying to others the speech component of DeCSS, the Appellants have not suggested, much less shown, any technique for barring them from making this instantaneous worldwide distribution of a decryption code that makes a lesser restriction on the code's speech component. It is true that the Government has alternative means of prohibiting unauthorized access to copyrighted materials. For example, it can create criminal and civil liability for those

who gain unauthorized access, and thus it can be argued that the restriction on posting DeCSS is not absolutely necessary to preventing unauthorized access to copyrighted materials. But a content-neutral regulation need not employ the least restrictive means of accomplishing the governmental objective. It need only avoid burdening "substantially more speech than is necessary to further the government's legitimate interests." The prohibition on the Defendants' posting of DeCSS satisfies that standard.

2. Linking

In considering linking, we need to clarify the sense in which the injunction prohibits such activity. . . . [T]he injunction . . . does not define "linking." Nevertheless, it is evident from the District Court's opinion that it is concerned with "hyperlinks." . . . The hyperlink can appear on a screen (window) as text, such as the Internet address ("URL") of the web page being called up or a word or phrase that identifies the web page to be called up, for example, "DeCSS web site." Or the hyperlink can appear as an image, for example, an icon depicting a person sitting at a computer watching a DVD movie and text stating "click here to access DeCSS and see DVD movies for free!" The code for the web page containing the hyperlink includes a computer instruction that associates the link with the URL of the web page to be accessed, such that clicking on the hyperlink instructs the computer to enter the URL of the desired web page and thereby access that page. With a hyperlink on a web page, the linked web site is just one click away.

In applying the DMCA to linking (via hyperlinks), Judge Kaplan recognized, as he had with DeCSS code, that a hyperlink has both a speech and a nonspeech component. It conveys information, the Internet address of the linked web page, and has the functional capacity to bring the content of the linked web page to the user's computer screen (or, as Judge Kaplan put it, to "take one almost instantaneously to the desired destination."). As he had ruled with respect to DeCSS code, he ruled that application of the DMCA to the Defendants' linking to web sites containing DeCSS is content-neutral. . . . The linking prohibition is justified solely by the functional capability of the hyperlink. . . .

Applying the *O'Brien*/*Ward*/*Turner Broadcasting* requirements for content-neutral regulation, Judge Kaplan then ruled that the DMCA, as applied to the Defendants' linking, served substantial governmental interests and was unrelated to the suppression of free expression. We agree. He then carefully considered the "closer call," as to whether a linking prohibition would satisfy the narrow tailoring requirement. In an especially carefully considered portion of his opinion, he observed that strict liability for linking to web sites containing DeCSS would risk two impairments of free expression. Web site operators would be inhibited from displaying links to various web pages for fear that a linked page might contain DeCSS, and a prohibition on linking to a web site containing DeCSS would curtail access to whatever other information was contained at the accessed site.

To avoid applying the DMCA in a manner that would "burden substantially more speech than is necessary to further the government's legitimate interests," Judge Kaplan adapted the standards of *New York Times Co. v. Sullivan* (1964), to fashion a limited prohibition against linking to web sites containing DeCSS. He required clear and convincing evidence

> that those responsible for the link (a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not lawfully be offered, and (c) create or maintain the link for the purpose of disseminating that technology.

He then found that the evidence satisfied his three-part test by his required standard of proof. . . .

Mindful of the cautious approach to First Amendment claims involving computer

technology expressed in *Name.Space*, we see no need on this appeal to determine whether a test as rigorous as Judge Kaplan's is required to respond to First Amendment objections to the linking provision of the injunction that he issued. It suffices to reject the Appellants' contention that an intent to cause harm is required and that linking can be enjoined only under circumstances applicable to a print medium. As they have throughout their arguments, the Appellants ignore the reality of the functional capacity of decryption computer code and hyperlinks to facilitate instantaneous unauthorized access to copyrighted materials by anyone anywhere in the world. Under the circumstances amply shown by the record, the injunction's linking prohibition validly regulates the Appellants' opportunity instantly to enable anyone anywhere to gain unauthorized access to copyrighted movies on DVDs.

At oral argument, we asked the Government whether its undoubted power to punish the distribution of obscene materials would permit an injunction prohibiting a newspaper from printing addresses of bookstore locations carrying such materials. In a properly cautious response, the Government stated that the answer would depend on the circumstances of the publication. The Appellants' supplemental papers enthusiastically embraced the arguable analogy between printing bookstore addresses and displaying on a web page links to web sites at which DeCSS may be accessed. They confidently asserted that publication of bookstore locations carrying obscene material cannot be enjoined consistent with the First Amendment, and that a prohibition against linking to web sites containing DeCSS is similarly invalid.

Like many analogies posited to illuminate legal issues, the bookstore analogy is helpful primarily in identifying characteristics that *distinguish* it from the context of the pending dispute. If a bookstore proprietor is knowingly selling obscene materials, the evil of distributing such materials can be prevented by injunctive relief against the unlawful distribution (and similar distribution by others can be deterred by punishment of the distributor). . . . The digital world, however, creates a very different problem. If obscene materials are posted on one web site and other sites post hyperlinks to the first site, the materials are available for instantaneous worldwide distribution before any preventive measures can be effectively taken.

This reality obliges courts considering First Amendment claims in the context of the pending case to choose between two unattractive alternatives: either tolerate some impairment of communication in order to permit Congress to prohibit decryption that may lawfully be prevented, or tolerate some decryption in order to avoid some impairment of communication. . . .

In facing this choice, we are mindful that it is not for us to resolve the issues of public policy implicated by the choice we have identified. Those issues are for Congress. Our task is to determine whether the legislative solution adopted by Congress, as applied to the Appellants by the District Court's injunction, is consistent with the limitations of the First Amendment, and we are satisfied that it is.

IV. Constitutional Challenge Based on Claimed Restriction of Fair Use

Asserting that fair use "is rooted in and required by both the Copyright Clause and the First Amendment," the Appellants contend that the DMCA, as applied by the District Court, unconstitutionally "*eliminates* fair use" of copyrighted materials (emphasis added). We reject this extravagant claim.

Preliminarily, we note that the Supreme Court has never held that fair use is constitutionally required, although some isolated statements in its opinions might arguably be enlisted for such a requirement. . . .

We need not explore the extent to which fair use might have constitutional

protection, grounded on either the First Amendment or the Copyright Clause, because whatever validity a constitutional claim might have as to an application of the DMCA that impairs fair use of copyrighted materials, such matters are far beyond the scope of this lawsuit for several reasons. In the first place, the Appellants do not claim to be making fair use of any copyrighted materials, and nothing in the injunction prohibits them from making such fair use. They are barred from trafficking in a decryption code that enables unauthorized access to copyrighted materials.

Second, as the District Court properly noted, to whatever extent the anti-trafficking provisions of the DMCA might prevent others from copying portions of DVD movies in order to make fair use of them, "the evidence as to the impact of the anti-trafficking provision[s] of the DMCA on prospective fair users is scanty and fails adequately to address the issues."

Third, the Appellants have provided no support for their premise that fair use of DVD movies is constitutionally required to be made by copying the original work in its original format. Their examples of the fair uses that they believe others will be prevented from making all involve copying in a digital format those portions of a DVD movie amenable to fair use, a copying that would enable the fair user to manipulate the digitally copied portions. One example is that of a school child who wishes to copy images from a DVD movie to insert into the student's documentary film. We know of no authority for the proposition that fair use, as protected by the Copyright Act, much less the Constitution, guarantees copying by the optimum method or in the identical format of the original. Although the Appellants insisted at oral argument that they should not be relegated to a "horse and buggy" technique in making fair use of DVD movies,[35] the DMCA does not impose even an arguable limitation on the opportunity to make a variety of traditional fair uses of DVD movies, such as commenting on their content, quoting excerpts from their screenplays, and even recording portions of the video images and sounds on film or tape by pointing a camera, a camcorder, or a microphone at a monitor as it displays the DVD movie. The fact that the resulting copy will not be as perfect or as manipulable as a digital copy obtained by having direct access to the DVD movie in its digital form, provides no basis for a claim of unconstitutional limitation of fair use. . . . Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original.

Conclusion

We have considered all the other arguments of the Appellants and conclude that they provide no basis for disturbing the District Court's judgment. Accordingly, the judgment is affirmed.

Questions:

1.) Why are Norwegian teenagers so good at hacking encryption systems? Long winter nights?

2.) Are you convinced that code is speech? If so, do you agree with the court's analysis of the First Amendment claim? If not, why not?

---

[35] In their supplemental papers, the Appellants contend, rather hyperbolically, that a prohibition on using copying machines to assist in making fair use of texts could not validly be upheld by the availability of "monks to scribe the relevant passages."

3.) What do you think of the Court's analysis of whether the DMCA unconstitutionally abridges fair use? If you were Corley's attorney, how would you have presented the argument? What if you were the attorney for Universal?

4.) How does the court reconcile its interpretation of 1201(a) with 1201(c)'s statement that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title"? Do you agree?

5.) The court did not reach the Constitutional argument that Section 1201 violates the IP clause's requirement that rights must be for "limited times." Why? Do you think there is an argument here? What if I add my copyrighted introduction to Shakespeare's sonnets and then (logically enough) encrypt the full eBook, so that circumventing in order to excerpt the public domain sonnets would run afoul of 1201(a); does this scenario raise constitutional concerns about "perpetual" copyright, or just involve matters of convenience and preferred format (anyone who wants the public domain sonnets should just buy another physical copy of them)? What if we reach the point when no one uses physical books anymore, and everything is only available on DRM-protected eBooks?

2.) Anti-Circumvention, Competition, and Consumer Choice

Chamberlain v. Skylink

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

GAJARSA, Circuit Judge.

Background

Chamberlain sued Skylink, alleging violations of the patent and copyright laws. . . . The matter on appeal involves only Chamberlain's allegation that Skylink is violating the DMCA, specifically the anti-trafficking provision of § 1201(a)(2). . . .

The technology at issue involves Garage Door Openers (GDOs). A GDO typically consists of a hand-held portable transmitter and a garage door opening device mounted in a homeowner's garage. The opening device, in turn, includes both a receiver with associated signal processing software and a motor to open or close the garage door. In order to open or close the garage door, a user must activate the transmitter, which sends a radio frequency (RF) signal to the receiver located on the opening device. Once the opener receives a recognized signal, the signal processing software directs the motor to open or close the garage door.

When a homeowner purchases a GDO system, the manufacturer provides both an opener and a transmitter. Homeowners who desire replacement or spare transmitters can

purchase them in the aftermarket. Aftermarket consumers have long been able to purchase "universal transmitters" that they can program to interoperate with their GDO system regardless of make or model. Skylink and Chamberlain are the only significant distributors of universal GDO transmitters. . . .

This dispute involves Chamberlain's Security+ line of GDOs and Skylink's Model 39 universal transmitter. Chamberlain's Security+ GDOs incorporate a copyrighted "rolling code" computer program that constantly changes the transmitter signal needed to open the garage door. Skylink's Model 39 transmitter, which does not incorporate rolling code, nevertheless allows users to operate Security+ openers. Chamberlain alleges that Skylink's transmitter renders the Security+ insecure by allowing unauthorized users to circumvent the security inherent in rolling codes. Of greater legal significance, however, Chamberlain contends that because of this property of the Model 39, Skylink is in violation of the anti-trafficking clause of the DMCA's anti-circumvention provisions, specifically § 1201(a)(2). . . .

Access and Protection

Congress crafted the new anti-circumvention and anti-trafficking provisions here at issue to help bring copyright law into the information age. Advances in digital technology over the past few decades have stripped copyright owners of much of the technological and economic protection to which they had grown accustomed. Whereas large-scale copying and distribution of copyrighted material used to be difficult and expensive, it is now easy and inexpensive. The *Reimerdes* court [*Reimerdes* is the District Court decision in *Corley*] correctly noted both the economic impact of these advances and their consequent potential impact on innovation. Congress therefore crafted legislation restricting some, but not all, technological measures designed either to access a work protected by copyright, § 1201(a), or to infringe a right of a copyright owner, § 1201(b).

Though as noted, circumvention *is not* a new form of infringement but rather a new violation prohibiting actions or products that facilitate infringement, it is significant that virtually every clause of § 1201 that mentions "access" links "access" to "protection." The import of that linkage may be less than obvious. Perhaps the best way to appreciate the necessity of this linkage—and the disposition of this case—is to consider three interrelated questions inherent in the DMCA's structure: What does § 1201(a)(2) prohibit above and beyond the prohibitions of § 1201(b)? What is the relationship between the sorts of "access" prohibited under § 1201(a) and the rights "protected" under the Copyright Act? and What is the relationship between anti-circumvention liability under § 1201(a)(1) and anti-trafficking liability under § 1201(a)(2)? The relationships among the new liabilities that these three provisions, §§ 1201(a)(1), (a)(2), (b), create circumscribe the DMCA's scope—and therefore allow us to determine whether or not Chamberlain's claim falls within its purview. And the key to disentangling these relationships lies in understanding the linkage between access and protection.

Chamberlain urges us to read the DMCA as if Congress simply created a new protection for copyrighted works without any reference at all either to the protections that copyright owners already possess or to the rights that the Copyright Act grants to the public. Chamberlain has not alleged that Skylink's Model 39 infringes its copyrights, nor has it alleged that the Model 39 contributes to third-party infringement of its copyrights. Chamberlain's allegation is considerably more straightforward: The only way for the Model 39 to interoperate with a Security+ GDO is by "accessing" copyrighted software. Skylink has therefore committed a *per se* violation of the DMCA. Chamberlain urges us to conclude that no necessary connection exists between access and *copyrights*. Congress

could not have intended such a broad reading of the DMCA.

Chamberlain derives its strongest claimed support for its proposed construction from the trial court's opinion in *Reimerdes*, [the earlier name for *Corley*] a case involving the same statutory provision. Though Chamberlain is correct in considering some of the *Reimerdes* language supportive, it is the differences between the cases, rather than their similarities, that is most instructive in demonstrating precisely what the DMCA permits and what it prohibits.

The facts here differ greatly from those in *Reimerdes*. There, a group of movie studios sought an injunction under the DMCA to prohibit illegal copying of digital versatile discs (DVDs). The plaintiffs presented evidence that each motion picture DVD includes a content scrambling system (CSS) that permits the film to be played, but not copied, using DVD players that incorporate the plaintiffs' licensed decryption technology. The defendant provided a link on his website that allowed an individual to download DeCSS, a program that allows the user to circumvent the CSS protective system and to view *or to copy* a motion picture from a DVD, whether or not the user has a DVD player with the licensed technology. The defendant proudly trumpeted his actions as "electronic civil disobedience." The court found that the defendant had violated 17 U.S.C. § 1201(a)(2)(A) because DeCSS had only one purpose: to decrypt CSS.

Chamberlain's proposed construction of the DMCA ignores the significant differences between defendants whose accused products enable copying and those, like Skylink, whose accused products enable only legitimate uses of copyrighted software . . . Many of Chamberlain's assertions in its brief to this court conflate the property right of copyright with the liability that the anti-circumvention provisions impose.

Chamberlain relies upon the DMCA's prohibition of "fair uses . . . as well as foul," *Reimerdes*, to argue that the enactment of the DMCA eliminated all existing consumer expectations about the public's rights to use purchased products because those products might include technological measures controlling access to a copyrighted work. But Chamberlain appears to have overlooked the obvious. The possibility that § 1201 might prohibit some otherwise noninfringing public uses of copyrighted material, arises simply because the Congressional decision to create liability and consequent damages for making, using, or selling a "key" that essentially enables a *trespass* upon intellectual property need not be identical in scope to the liabilities and compensable damages for *infringing* that property; it is, instead, a rebalancing of interests that "attempt[s] to deal with special problems created by the so-called digital revolution."

Though *Reimerdes* is not the only case that Chamberlain cites for support, none of its other citations are any more helpful to its cause. In three other cases, *Lexmark International, Inc. v. Static Control Components, Inc.* (E.D. Ky. 2003), *Sony Computer Entertainment America, Inc. v. Gamemasters* (N.D. Cal. 1999), and *RealNetworks* (2000), the trial courts did grant preliminary injunctions under the DMCA using language supportive of Chamberlain's proposed construction. None of these cases, however, is on point. In *Lexmark*, the trial court ruled that the defendant's conduct constituted copyright infringement. In *Sony*, the plaintiff's allegations included both trademark and copyright infringement, and the defendant conceded that its product made "temporary modifications" to the plaintiff's copyrighted computer program. In *RealNetworks*, the defendant's product allegedly disabled RealNetworks' "copy switch," RealNetworks' technological measure designed to let the owner of copyrighted material being streamed over RealNetworks' media player either enable or disable copying upon streaming. The court stated explicitly that the avoidance of the copy switch appeared to have little commercial value other than circumvention and the consequent infringement that it enabled. In short, the access alleged in all three cases was

intertwined with a protected right. None of these cases can support a construction as broad as the one that Chamberlain urges us to adopt, even as persuasive authority.

Furthermore, though the severance of access from protection appears plausible taken out of context, it would also introduce a number of irreconcilable problems in statutory construction. The seeming plausibility arises because the statute's structure could be seen to suggest that § 1201(b) strengthens a copyright owner's abilities to protect its recognized *rights*, while § 1201(a) strengthens a copyright owner's abilities to protect *access* to its work without regard to the legitimacy (or illegitimacy) of the actions that the accused access enables. Such an interpretation is consistent with the Second Circuit's description: "[T]he focus of subsection 1201(a)(2) is circumvention of technologies designed to *prevent access* to a work, and the focus of subsection 1201(b)(1) is circumvention of technologies designed to *permit access* to a work but *prevent copying* of the work or some other act that infringes a copyright." *Corley*.

It is unlikely, however, that the Second Circuit meant to imply anything as drastic as wresting the concept of "access" from its context within the Copyright Act, as Chamberlain would now have us do. Were § 1201(a) to allow copyright owners to use technological measures to block *all* access to their copyrighted works, it would effectively create two distinct copyright regimes. In the first regime, the owners of a typical work protected by copyright would possess only the rights enumerated in 17 U.S.C. § 106, subject to the additions, exceptions, and limitations outlined throughout the rest of the Copyright Act—notably but not solely the fair use provisions of § 107.[14] Owners who feel that technology has put those rights at risk, and who incorporate technological measures to protect those rights from technological encroachment, gain the additional ability to hold traffickers in circumvention devices liable under § 1201(b) for putting their rights back at risk by enabling circumventors who use these devices to infringe.

Under the second regime that Chamberlain's proposed construction implies, the owners of a work protected by *both* copyright *and* a technological measure that effectively controls access to that work per § 1201(a) would possess *unlimited* rights to hold circumventors liable under § 1201(a) *merely for accessing that work*, even if that access enabled *only* rights that the Copyright Act grants to the public. This second implied regime would be problematic for a number of reasons. First, as the Supreme Court recently explained, "Congress' exercise of its Copyright Clause authority must be rational." *Eldred v. Ashcroft* (2003). In determining whether a particular aspect of the Copyright Act "is a rational exercise of the legislative authority conferred by the Copyright Clause . . . we defer substantially to Congress. It is Congress that has been assigned the task of defining the scope of the limited monopoly that should be granted to authors . . . *in order to give the public appropriate access* to their work product." Chamberlain's proposed construction of § 1201(a) implies that in enacting the DMCA, Congress attempted to "give the public appropriate access" to copyrighted works by allowing copyright owners to deny all access to the public. Even under the substantial deference due Congress, such a redefinition borders on the irrational.

That apparent irrationality, however, is not the most significant problem that this second regime implies. Such a regime would be hard to reconcile with the DMCA's

---

[14] We do not reach the relationship between § 107 fair use and violations of § 1201. The District Court in *Reimerdes* rejected the DeCSS defendants' argument that fair use was a *necessary* defense to § 1201(a); because any access enables some fair uses, *any* act of circumvention would embody its own defense. We leave open the question as to when § 107 might serve as an affirmative defense to a prima facie violation of § 1201. For the moment, we note only that though the traditional fair use doctrine of § 107 remains unchanged as a defense to copyright infringement under § 1201(c)(1), circumvention is not infringement.

statutory prescription that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." 17 U.S.C. § 1201(c)(1). A provision that prohibited access without regard to the rest of the Copyright Act would clearly affect rights and limitations, if not remedies and defenses. Justice Souter has remarked that "[n]o canon of statutory construction familiar to me specifically addresses the situation in which two simultaneously enacted provisions of the same statute flatly contradict one another. We are, of course, bound to avoid such a dilemma if we can, by glimpsing some uncontradicted meaning for each provision." *Reno v. American-Arab Anti-Discrimination Comm.* (1999) (Souter, J., dissenting). Chamberlain's proposed construction of § 1201(a) would flatly contradict § 1201(c)(1)—a simultaneously enacted provision of the same statute. We are therefore bound, if we can, to obtain an alternative construction that leads to no such contradiction.

Chamberlain's proposed severance of "access" from "protection" in § 1201(a) creates numerous other problems. Beyond suggesting that Congress enacted *by implication* a new, highly protective alternative regime for copyrighted works; contradicting other provisions of the same statute including § 1201(c)(1); and ignoring the explicit immunization of interoperability from anti-circumvention liability under § 1201(f); the broad policy implications of considering "access" in a vacuum devoid of "protection" are both absurd and disastrous. Under Chamberlain's proposed construction, explicated at oral argument, disabling a burglar alarm to gain "access" to a home containing copyrighted books, music, art, and periodicals would violate the DMCA; anyone who did so would unquestionably have "circumvent[ed] a technological measure that effectively controls access to a work protected under [the Copyright Act]." § 1201(a)(1). The appropriate deterrents to this type of behavior lie in tort law and criminal law, *not* in copyright law. Yet, were we to read the statute's "plain language" as Chamberlain urges, disabling a burglar alarm would be a per se violation of the DMCA.

In a similar vein, Chamberlain's proposed construction would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial "encryption" scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products. In other words, Chamberlain's construction of the DMCA would allow virtually any company to attempt to leverage its sales into aftermarket monopolies—a practice that both the antitrust laws, and the doctrine of copyright misuse, normally prohibit.

Even were we to assume *arguendo* that the DMCA's anti-circumvention provisions created a new property right, Chamberlain's attempt to infer such an exemption from copyright misuse and antitrust liability would *still* be wrong. We have noted numerous times that as a matter of Federal Circuit law, "[i]ntellectual property rights do not confer a privilege to violate the antitrust laws. But it is also correct that the antitrust laws do not negate [a] patentee's right to exclude others from patent property." *CSU, L.L.C. v. Xerox Corp.* (Fed. Cir. 2000). In what we previously termed "the most extensive analysis of the effect of a unilateral refusal to license copyrighted expression," among our sister Circuits, the First Circuit explained that: "[T]he Copyright Act does not explicitly purport to limit the scope of the Sherman Act. . . . [W]e must harmonize the two [Acts] as best we can." *Data Gen. Corp. v. Grumman Sys. Support Corp.* (1st Cir. 1994).

Because nothing in Seventh Circuit law contradicts *Data General*, we similarly conclude that it is the standard that the Seventh Circuit would most likely follow. The DMCA, as part of the Copyright Act, does not limit the scope of the antitrust laws, either explicitly or implicitly. The Supreme Court

> has considered the issue of implied repeal of the antitrust laws in the

> context of a variety of regulatory schemes and procedures. Certain axioms of construction are now clearly established. Repeal of the antitrust laws by implication is not favored and not casually to be allowed. Only where there is a plain repugnancy between the antitrust and regulatory provisions will repeal be implied.

Gordon v. N.Y. Stock Exch., Inc. (1975). . . .

Finally, the requisite "authorization," on which the District Court granted Skylink summary judgment, points to yet another inconsistency in Chamberlain's proposed construction. . . . Underlying Chamberlain's argument on appeal that it has not granted such authorization lies the necessary assumption that Chamberlain is entitled to prohibit legitimate purchasers of its embedded software from "accessing" the software by using it. Such an entitlement, however, would go far beyond the idea that the DMCA allows copyright owner to prohibit "fair uses . . . as well as foul." Chamberlain's proposed construction would allow copyright owners to prohibit *exclusively fair* uses even in the absence of any feared foul use. It would therefore allow any copyright owner, through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work—or even selected copies of that copyrighted work. Again, this implication contradicts § 1201(c)(1) directly. Copyright law itself authorizes the public to make certain uses of copyrighted materials. Consumers who purchase a product containing a copy of embedded software have the inherent legal right to use that copy of the software. What the law authorizes, Chamberlain cannot revoke.[17]

Chamberlain's proposed severance of "access" from "protection" is entirely inconsistent with the context defined by the total statutory structure of the Copyright Act, other simultaneously enacted provisions of the DMCA, and clear Congressional intent. It "would lead to a result so bizarre that Congress could not have intended it." The statutory structure and the legislative history both make it clear that the DMCA granted copyright holders additional legal protections, but neither rescinded the basic bargain granting the public noninfringing and fair uses of copyrighted materials, § 1201(c), nor prohibited various beneficial uses of circumvention technology, such as those exempted under §§ 1201(d),(f),(g),(j).

We therefore reject Chamberlain's proposed construction in its entirety. We conclude that 17 U.S.C. § 1201 prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners. While such a rule of reason may create some uncertainty and consume some judicial resources, it is the only meaningful reading of the statute. Congress attempted to balance the legitimate interests of copyright owners with those of consumers of copyrighted products. . . .

Congress chose words consistent with its stated intent to balance two sets of concerns pushing in opposite directions. The statute lays out broad categories of liability and broad exemptions from liability. It also instructs the courts explicitly *not* to construe the anti-circumvention provisions in ways that would effectively repeal longstanding principles of copyright law. *See* § 1201(c). The courts must decide where the balance between the rights of copyright owners and those of the broad public tilts subject to a fact-specific rule of reason. Here, Chamberlain can point to no protected property right

---

[17] It is not clear whether a consumer who circumvents a technological measure controlling access to a copyrighted work in a manner that enables uses permitted under the Copyright Act but prohibited by contract can be subject to liability under the DMCA. Because Chamberlain did not attempt to limit its customers' use of its product by contract, however, we do not reach this issue.

that Skylink imperils. The DMCA cannot allow Chamberlain to retract the most fundamental right that the Copyright Act grants consumers: the right to use the copy of Chamberlain's embedded software that they purchased.

Chamberlain's DMCA Claim

The proper construction of § 1201(a)(2) therefore makes it clear that Chamberlain cannot prevail. A plaintiff alleging a violation of § 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure. A plaintiff incapable of establishing any one of elements (1) through (5) will have failed to prove a prima facie case. A plaintiff capable of proving elements (1) through (5) need prove only one of (6)(i), (ii), or (iii) to shift the burden back to the defendant. At that point, the various affirmative defenses enumerated throughout § 1201 become relevant. . . .

Questions:

1.) Is *Skylink* consistent with *Corley*? Why or why not?

2.) Do you agree with the *Skylink* court's "nexus" requirement? Explain its reasoning. Are there other grounds on which the court could have ruled for Skylink?

3.) If *Skylink*'s interpretation of § 1201 is correct, can you provide an example of a violation of § 1201(a)(2) that is not also a violation of § 1201(b)? What would the *Skylink* court say is the purpose of having *both* anti-trafficking provisions?

PROBLEM 15-1

Look back at Problem 12-1. If you recall, a neighborhood bookstore had on display a mint-condition, unopened copy of Madonna's 1992 book *Sex*, which was sealed with a paper band. On the paper band was an announcement that breaking the band constituted a promise to buy, and that doing so without paying constituted copyright infringement. James broke the band, peeked inside the book, and left the store without buying it. Did James infringe copyright?

Now a few years have passed and James is raising tweenage girls who are huge fans of Miley Cyrus and Lady Gaga. He has become increasingly disturbed by the provocative behavior of these recording artists and how it is influencing his daughters. He concludes that overt sexuality in female recording stars can be traced back to a single source—Madonna's book. He decides that the most effective way of de-twerking popular culture is to create a powerful parody of this book. James finds an eBook version of *Sex* on the internet, but it is encrypted, and he cannot get an access code without paying for it. He refuses to support such depravity financially. Instead, he uses Jennifer's "FairXTract" program to decrypt the eBook and extract a small amount of text and imagery for his parody.

FairXTract is a popular open source program that can convert DRM encrypted text

and image files into more open formats that can be freely read, copied or edited without restriction. The program is made available freely online and lists a number of possible uses: "Make backup copies of your e-library! Don't be locked in to your obsolete e-reader! Annotate and comment on your favorite literature. Create excerpts for your English class. FairXTract is the key to FairXUse!" James's parody, "(Im)material Girl," portrays Madonna's musings on sexuality as the cynical objectification of female sexuality in the service of profit. He posts it on his blog, "Family Values—A Return to Decency." Assume that his parody would be considered a fair use under § 107.

Has James violated the DMCA? Has Jennifer? If so, what provisions have they violated? How would the *Corley* court hold? What about the *Skylink* court?

3.) The Interaction between Copyright, Contracts, and the DMCA

MDY Industries, LLC v. Blizzard Entertainment, Inc.

629 F.3d 928 (9th Cir. 2010)

CALLAHAN, Circuit Judge.

Blizzard Entertainment, Inc. ("Blizzard") is the creator of World of Warcraft ("WoW"), a popular multiplayer online role-playing game in which players interact in a virtual world while advancing through the game's 70 levels. MDY Industries, LLC and its sole member Michael Donnelly ("Donnelly") (. . . "MDY") developed and sold Glider, a software program that automatically plays the early levels of WoW for players.

MDY brought this action for a declaratory judgment to establish that its Glider sales do not infringe Blizzard's copyright or other rights, and Blizzard asserted counterclaims under the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 *et seq.*, and for tortious interference with contract under Arizona law. The district court found MDY and Donnelly liable for secondary copyright infringement, violations of DMCA §§ 1201(a)(2) and (b)(1), and tortious interference with contract. We reverse the district court except as to MDY's liability for violation of DMCA § 1201(a)(2) and remand for trial on

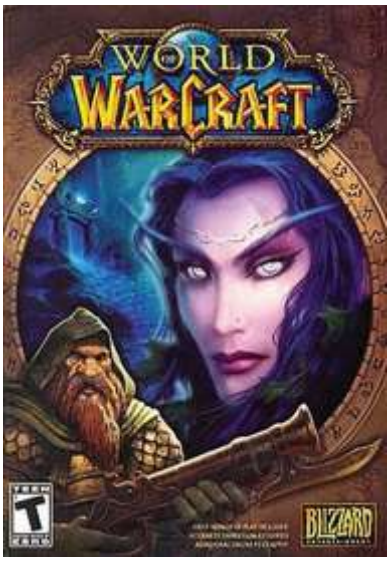

Image information available at http://en.wikipedia.org/wiki/File:WoW_Box_Art1.jpg.

Blizzard's claim for tortious interference with contract.

I.

A. World of Warcraft

In November 2004, Blizzard created WoW, a "massively multiplayer online role-playing game" in which players interact in a virtual world. WoW has ten million subscribers, of which two and a half million are in North America. The WoW software has two components: (1) the game client software that a player installs on the computer; and (2) the game server software, which the player accesses on a subscription basis by connecting to WoW's online servers. WoW does not have single-player or offline modes.

WoW players roleplay different characters, such as humans, elves, and dwarves. A player's central objective is to advance the character through the game's 70 levels by participating in quests and engaging in battles with monsters. As a player advances, the character collects rewards such as ingame currency, weapons, and armor. WoW's virtual world has its own economy, in which characters use their virtual currency to buy and sell items directly from each other, through vendors, or using auction houses. Some players also utilize WoW's chat capabilities to interact with others.

B. Blizzard's use agreements

Each WoW player must read and accept Blizzard's End User License Agreement ("EULA") and Terms of Use ("ToU") on multiple occasions. The EULA pertains to the game client, so a player agrees to it both before installing the game client and upon first running it. The ToU pertains to the online service, so a player agrees to it both when creating an account and upon first connecting to the online service. Players who do not accept both the EULA and the ToU may return the game client for a refund.

C. Development of Glider and Warden

Donnelly is a WoW player and software programmer. In March 2005, he developed Glider, a software "bot" (short for robot) that automates play of WoW's early levels, for his personal use. A user need not be at the computer while Glider is running. As explained in the Frequently Asked Questions ("FAQ") on MDY's website for Glider:

> Glider . . . moves the mouse around and pushes keys on the keyboard. You tell it about your character, where you want to kill things, and when you want to kill. Then it kills for you, automatically. You can do something else, like eat dinner or go to a movie, and when you return, you'll have a lot more experience and loot.

Glider does not alter or copy WoW's game client software, does not allow a player to avoid paying monthly subscription dues to Blizzard, and has no commercial use independent of WoW. Glider was not initially designed to avoid detection by Blizzard.

The parties dispute Glider's impact on the WoW experience. Blizzard contends that Glider disrupts WoW's environment for non-Glider players by enabling Glider users to advance quickly and unfairly through the game and to amass additional game assets. MDY contends that Glider has a minimal effect on non-Glider players, enhances the WoW experience for Glider users, and facilitates disabled players' access to WoW by auto-playing the game for them.

In summer 2005, Donnelly began selling Glider through MDY's website for fifteen to twenty-five dollars per license. . . . In September 2005, Blizzard launched Warden, a technology that it developed to prevent its players who use unauthorized third-party software, including bots, from connecting to WoW's servers. Warden was able to detect

Glider, and Blizzard immediately used Warden to ban most Glider users. MDY responded by modifying Glider to avoid detection and promoting its new anti-detection features on its website's FAQ. It added a subscription service, Glider Elite, which offered "additional protection from game detection software" for five dollars a month.

Thus, by late 2005, MDY was aware that Blizzard was prohibiting bots. MDY modified its website to indicate that using Glider violated Blizzard's ToU. In November 2005, Donnelly wrote in an email interview, "Avoiding detection is rather exciting, to be sure. Since Blizzard does not want bots running at all, it's a violation to use them." Following MDY's anti-detection modifications, Warden only occasionally detected Glider. As of September 2008, MDY had gross revenues of $3.5 million based on 120,000 Glider license sales.

D. Financial and practical impact of Glider

Blizzard claims that from December 2004 to March 2008, it received 465,000 complaints about WoW bots, several thousand of which named Glider. Blizzard spends $940,000 annually to respond to these complaints, and the parties have stipulated that Glider is the principal bot used by WoW players. Blizzard introduced evidence that it may have lost monthly subscription fees from Glider users, who were able to reach WoW's highest levels in fewer weeks than players playing manually. Donnelly acknowledged in a November 2005 email that MDY's business strategy was to make Blizzard's anti-bot detection attempts financially prohibitive. . . .

E. Pre-litigation contact between MDY and Blizzard

In August 2006, Blizzard sent MDY a cease-and-desist letter alleging that MDY's website hosted WoW screenshots and a Glider install file, all of which infringed Blizzard's copyrights. Donnelly removed the screenshots and requested Blizzard to clarify why the install file was infringing, but Blizzard did not respond. In October 2006, Blizzard's counsel visited Donnelly's home, threatening suit unless MDY immediately ceased selling Glider and remitted all profits to Blizzard. MDY immediately commenced this action.

II.

On December 1, 2006, MDY filed an amended complaint seeking a declaration that Glider does not infringe Blizzard's copyright or other rights. In February 2007, Blizzard filed counterclaims and third-party claims against MDY and Donnelly for, *inter alia*, contributory and vicarious copyright infringement, violation of DMCA §§ 1201(a)(2) and (b)(1), and tortious interference with contract.

In July 2008, the district court granted Blizzard partial summary judgment, finding that MDY's Glider sales contributorily and vicariously infringed Blizzard's copyrights and tortiously interfered with Blizzard's contracts. The district court also granted MDY partial summary judgment, finding that MDY did not violate DMCA § 1201(a)(2) with respect to accessing the game software's source code.

In September 2008, the parties stipulated to entry of a $6 million judgment against MDY for the copyright infringement and tortious interference with contract claims. They further stipulated that Donnelly would be personally liable for the same amount if found personally liable at trial. After a January 2009 bench trial, the district court held MDY liable under DMCA §§ 1201(a)(2) and (b)(1). It also held Donnelly personally liable for MDY's copyright infringement, DMCA violations, and tortious interference with contract.

. . . The district court permanently enjoined MDY from distributing Glider. MDY's efforts to stay injunctive relief pending appeal were unsuccessful. On April 29, 2009,

MDY timely filed this appeal. On May 12, 2009, Blizzard timely cross-appealed the district court's holding that MDY did not violate DMCA §§ 1201(a)(2) and (b)(1) as to the game software's source code. . . .

IV.

We first consider whether MDY committed contributory or vicarious infringement (collectively, "secondary infringement") of Blizzard's copyright by selling Glider to WoW players. *See ProCD, Inc. v. Zeidenberg* (7th Cir. 1996) ("A copyright is a right against the world. Contracts, by contrast, generally affect only their parties."). To establish secondary infringement, Blizzard must first demonstrate direct infringement. To establish direct infringement, Blizzard must demonstrate copyright ownership and violation of one of its exclusive rights by Glider users. MDY is liable for contributory infringement if it has "intentionally induc[ed] or encourag[ed] direct infringement" by Glider users. *MGM Studios Inc. v. Grokster, Ltd.* (2005). MDY is liable for vicarious infringement if it (1) has the right and ability to control Glider users' putatively infringing activity and (2) derives a direct financial benefit from their activity. If Glider users directly infringe, MDY does not dispute that it satisfies the other elements of contributory and vicarious infringement.

As a copyright owner, Blizzard possesses the exclusive right to reproduce its work. 17 U.S.C. § 106(1). The parties agree that when playing WoW, a player's computer creates a copy of the game's software in the computer's random access memory ("RAM"), a form of temporary memory used by computers to run software programs. This copy potentially infringes unless the player (1) is a licensee whose use of the software is within the scope of the license or (2) owns the copy of the software. 17 U.S.C. § 117(a). As to the scope of the license, ToU § 4(B), "Limitations on Your Use of the Service," provides:

> You agree that you will not . . . (ii) create or use cheats, bots, "mods," and/or hacks, or any other third-party software designed to modify the World of Warcraft experience; or (iii) use any third-party software that intercepts, "mines," or otherwise collects information from or through the Program or Service.

By contrast, if the player owns the copy of the software, the "essential step" defense provides that the player does not infringe by making a copy of the computer program where the copy is created and used solely "as an essential step in the utilization of the computer program in conjunction with a machine." 17 U.S.C. § 117(a)(1).

A. Essential step defense

We consider whether WoW players, including Glider users, are owners or licensees of their copies of WoW software. If WoW players own their copies, as MDY contends, then Glider users do not infringe by reproducing WoW software in RAM while playing, and MDY is not secondarily liable for copyright infringement.

In *Vernor v. Autodesk, Inc.*, we recently distinguished between "owners" and "licensees" of copies for purposes of the essential step defense. In *Vernor*, we held "that a software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use" restrictions.

Applying *Vernor*, we hold that WoW players are licensees of WoW's game client software. Blizzard reserves title in the software and grants players a non-exclusive, limited license. Blizzard also imposes transfer restrictions if a player seeks to transfer the license: the player must (1) transfer all original packaging and documentation; (2) permanently

delete all of the copies and installation of the game client; and (3) transfer only to a recipient who accepts the EULA. A player may not sell or give away the account.

Blizzard also imposes a variety of use restrictions. The game must be used only for non-commercial entertainment purposes and may not be used in cyber cafes and computer gaming centers without Blizzard's permission. Players may not concurrently use unauthorized third-party programs. Also, Blizzard may alter the game client itself remotely without a player's knowledge or permission, and may terminate the EULA and ToU if players violate their terms. Termination ends a player's license to access and play WoW. Following termination, players must immediately destroy their copies of the game and uninstall the game client from their computers, but need not return the software to Blizzard.

Since WoW players, including Glider users, do not own their copies of the software, Glider users may not claim the essential step defense. Thus, when their computers copy WoW software into RAM, the players may infringe unless their usage is within the scope of Blizzard's limited license.

B. Contractual covenants vs. license conditions

"A copyright owner who grants a nonexclusive, limited license ordinarily waives the right to sue licensees for copyright infringement, and it may sue only for breach of contract." However, if the licensee acts outside the scope of the license, the licensor may sue for copyright infringement. Enforcing a copyright license "raises issues that lie at the intersection of copyright and contract law."

We refer to contractual terms that limit a license's scope as "conditions," the breach of which constitute copyright infringement. We refer to all other license terms as "covenants," the breach of which is actionable only under contract law. We distinguish between conditions and covenants according to state contract law, to the extent consistent with federal copyright law and policy.

A Glider user commits copyright infringement by playing WoW while violating a ToU term that is a license condition. To establish copyright infringement, then, Blizzard must demonstrate that the violated term—ToU § 4(B)—is a condition rather than a covenant. Blizzard's EULAs and ToUs provide that they are to be interpreted according to Delaware law. Accordingly, we first construe them under Delaware law, and then evaluate whether that construction is consistent with federal copyright law and policy.

A covenant is a contractual promise, i.e., a manifestation of intention to act or refrain from acting in a particular way, such that the promisee is justified in understanding that the promisor has made a commitment. A condition precedent is an act or event that must occur before a duty to perform a promise arises. Conditions precedent are disfavored because they tend to work forfeitures. Wherever possible, equity construes ambiguous contract provisions as covenants rather than conditions. However, if the contract is unambiguous, the court construes it according to its terms.

Applying these principles, ToU § 4(B)(ii) and (iii)'s prohibitions against bots and unauthorized third-party software are covenants rather than copyright-enforceable conditions. Although ToU § 4 is titled, "Limitations on Your Use of the Service," nothing in that section conditions Blizzard's grant of a limited license on players' compliance with ToU § 4's restrictions. To the extent that the title introduces any ambiguity, under Delaware law, ToU § 4(B) is not a condition, but is a contractual covenant.

To recover for copyright infringement based on breach of a license agreement, (1) the copying must exceed the scope of the defendant's license and (2) the copyright owner's complaint must be grounded in an exclusive right of copyright (e.g., unlawful reproduction or distribution). Contractual rights, however, can be much broader:

> [C]onsider a license in which the copyright owner grants a person the right to make one and only one copy of a book with the caveat that the licensee may not read the last ten pages. Obviously, a licensee who made a hundred copies of the book would be liable for copyright infringement because the copying would violate the Copyright Act's prohibition on reproduction and would exceed the scope of the license. Alternatively, if the licensee made a single copy of the book, but read the last ten pages, the only cause of action would be for breach of contract, because reading a book does not violate any right protected by copyright law.

Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc. (Fed. Cir. 2005). Consistent with this approach, we have held that the potential for infringement exists only where the licensee's action (1) exceeds the license's scope (2) in a manner that implicates one of the licensor's exclusive statutory rights.

Here, ToU § 4 contains certain restrictions that are grounded in Blizzard's exclusive rights of copyright and other restrictions that are not. For instance, ToU § 4(D) forbids creation of derivative works based on WoW without Blizzard's consent. A player who violates this prohibition would exceed the scope of her license and violate one of Blizzard's exclusive rights under the Copyright Act. In contrast, ToU § 4(C)(ii) prohibits a player's disruption of another player's game experience. A player might violate this prohibition while playing the game by harassing another player with unsolicited instant messages. Although this conduct may violate the contractual covenants with Blizzard, it would not violate any of Blizzard's exclusive rights of copyright. The antibot provisions at issue in this case, ToU § 4(B)(ii) and (iii), are similarly covenants rather than conditions. A Glider user violates the covenants with Blizzard, but does not thereby commit copyright infringement because Glider does not infringe any of Blizzard's exclusive rights. For instance, the use does not alter or copy WoW software.

Were we to hold otherwise, Blizzard—or any software copyright holder—could designate any disfavored conduct during software use as copyright infringement, by purporting to condition the license on the player's abstention from the disfavored conduct. The rationale would be that because the conduct occurs while the player's computer is copying the software code into RAM in order for it to run, the violation is copyright infringement. This would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners.[3]

We conclude that for a licensee's violation of a contract to constitute copyright infringement, there must be a nexus between the condition and the licensor's exclusive rights of copyright. Here, WoW players do not commit copyright infringement by using Glider in violation of the ToU. MDY is thus not liable for secondary copyright infringement, which requires the existence of direct copyright infringement.

It follows that because MDY does not infringe Blizzard's copyrights, we need not resolve MDY's contention that Blizzard commits copyright misuse. Copyright misuse is an equitable defense to copyright infringement, the contours of which are still being defined. The remedy for copyright misuse is to deny the copyright holder the right to

---

[3] A copyright holder may wish to enforce violations of license agreements as copyright infringements for several reasons. First, breach of contract damages are generally limited to the value of the actual loss caused by the breach. In contrast, copyright damages include the copyright owner's actual damages and the infringer's actual profits, or statutory damages of up to $150,000 per work. 17 U.S.C. § 504. Second, copyright law offers injunctive relief, seizure of infringing articles, and awards of costs and attorneys' fees. 17 U.S.C. §§ 502–03, 505. Third, . . . copyright law allows copyright owners a remedy against "downstream" infringers with whom they are not in privity of contract.

enforce its copyright during the period of misuse. Since MDY does not infringe, we do not consider whether Blizzard committed copyright misuse.

We thus reverse the district court's grant of summary judgment to Blizzard on its secondary copyright infringement claims. . . .

V.

After MDY began selling Glider, Blizzard launched Warden, its technology designed to prevent players who used bots from connecting to the WoW servers. Blizzard used Warden to ban most Glider users in September 2005. Blizzard claims that MDY is liable under DMCA §§ 1201(a)(2) and (b)(1) because it thereafter programmed Glider to avoid detection by Warden.

A. The Warden technology

Warden has two components. The first is a software module called "scan.dll," which scans a computer's RAM prior to allowing the player to connect to WoW's servers. If scan.dll detects that a bot is running, such as Glider, it will not allow the player to connect and play. After Blizzard launched Warden, MDY reconfigured Glider to circumvent scan.dll by not loading itself until after scan.dll completed its check. Warden's second component is a "resident" component that runs periodically in the background on a player's computer when it is connected to WoW's servers. It asks the computer to report portions of the WoW code running in RAM, and it looks for patterns of code associated with known bots or cheats. If it detects a bot or cheat, it boots the player from the game, which halts the computer's copying of copyrighted code into RAM.

B. The Digital Millennium Copyright Act

. . . The first provision, 17 U.S.C. § 1201(a)(1)(A), is a general prohibition against "circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act]." The second prohibits trafficking in technology that circumvents a technological measure that "effectively controls access" to a copyrighted work. 17 U.S.C. § 1201(a)(2). The third prohibits trafficking in technology that circumvents a technological measure that "effectively protects" a copyright owner's right. 17 U.S.C. § 1201(b)(1).

C. The district court's decision

The district court assessed whether MDY violated DMCA §§ 1201(a)(2) and (b)(1) with respect to three WoW components. First, the district court considered the game client software's **literal elements**: the source code stored on players' hard drives. Second, the district court considered the game client software's **individual non-literal elements**: the 400,000+ discrete visual and audible components of the game, such as a visual image of a monster or its audible roar. Finally, it considered the game's **dynamic non-literal elements**: that is, the "real-time experience of traveling through different worlds, hearing their sounds, viewing their structures, encountering their inhabitants and monsters, and encountering other players."

The district court granted MDY partial summary judgment as to Blizzard's § 1201(a)(2) claim with respect to WoW's literal elements. The district court reasoned that Warden does not effectively control access to the literal elements because WoW players can access the literal elements without connecting to a game server and encountering Warden; they need only install the game client software on their computers. The district court also ruled for MDY following trial as to Blizzard's § 1201(a)(2) claim with respect to WoW's

individual non-literal elements, reasoning that these elements could also be accessed on a player's hard drive without encountering Warden. . . . The district court, however, ruled for Blizzard following trial as to its §§ 1201(a)(2) and (b)(1) claims with respect to WoW's dynamic non-literal elements, or the "real-time experience" of playing WoW. . . .

We turn to consider whether Glider violates DMCA §§ 1201(a)(2) and (b)(1) by allowing users to circumvent Warden to access WoW's various elements. MDY contends that Warden's scan.dll and resident components are separate, and only scan.dll should be considered as a potential access control measure under § 1201(a)(2). However, in our view, an access control measure can both (1) attempt to block initial access and (2) revoke access if a secondary check determines that access was unauthorized. Our analysis considers Warden's scan.dll and resident components together because the two components have the same purpose: to prevent players using detectable bots from continuing to access WoW software.

D. Construction of § 1201

One of the issues raised by this appeal is whether certain provisions of § 1201 prohibit circumvention of access controls when access does not constitute copyright infringement. To answer this question and others presented by this appeal, we address the nature and interrelationship of the various provisions of § 1201 in the overall context of the Copyright Act.

We begin by considering the scope of DMCA § 1201's three operative provisions, §§ 1201(a)(1), 1201(a)(2), and 1201(b)(1). We consider them side-by-side, because "[w]e do not . . . construe statutory phrases in isolation; we read statutes as a whole. Thus, the [term to be construed] must be read in light of the immediately following phrase . . . ."

1. Text of the operative provisions

"We begin, as always, with the text of the statute." Section 1201(a)(1)(A) prohibits "circumvent[ing] a technological measure that effectively controls access to a work protected under this title." Sections 1201(a)(2) and (b)(1) provide that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —

§ 1201(a)(2)	§ 1201(b)(1)
(A) is primarily designed or produced for the purpose of **circumventing a technological measure** that effectively controls access to **a work protected under this title;**	(A) is primarily designed or produced for the purpose of **circumventing protection afforded** **by a technological measure** that effectively protects **a right of a copyright owner;**
(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title;	(B) has only limited commercially significant purpose of use other than to circumvent protection afforded by a a technological measure that effectively protects a right of a copyright owner under this title in a work or portion thereof;
(C) is marked by a person or another acting in concert with that person	(C) is marketed by that person or another acting in concert with that person

with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.	with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a portion or work thereof."

(emphasis added).

2. Our harmonization of the DMCA's operative provisions

For the reasons set forth below, we believe that § 1201 is best understood to create two distinct types of claims. First, § 1201(a) prohibits the circumvention of any technological measure that effectively controls access to a protected work and grants copyright owners the right to enforce that prohibition. *Cf. Corley* ("[T]he focus of subsection 1201(a)(2) is circumvention of technologies designed to prevent access to a work"). Second, and in contrast to § 1201(a), § 1201(b)(1) prohibits trafficking in technologies that circumvent technological measures that effectively protect "a right of a copyright owner." Section 1201(b)(1)'s prohibition is thus aimed at circumventions of measures that protect the copyright itself: it entitles copyright owners to protect their existing exclusive rights under the Copyright Act. Those exclusive rights are reproduction, distribution, public performance, public display, and creation of derivative works. 17 U.S.C. § 106. Historically speaking, preventing "access" to a protected work in itself has not been a right of a copyright owner arising from the Copyright Act.

Our construction of § 1201 is compelled by the four significant textual differences between §§ 1201(a) and (b). First, § 1201(a)(2) prohibits the circumvention of a measure that "effectively controls access to *a work protected under this title*," whereas § 1201(b)(1) concerns a measure that "effectively protects *a right of a copyright owner under this title in a work or portion thereof*." We read § 1201(b)(1)'s language—"right of a copyright owner under this title"—to reinforce copyright owners' traditional exclusive rights under § 106 by granting them an additional cause of action against those who traffic in circumventing devices that facilitate infringement. Sections 1201(a)(1) and (a)(2), however, use the term "work protected under this title." Neither of these two subsections explicitly refers to traditional copyright infringement under § 106. Accordingly, we read this term as extending a new form of protection, i.e., the right to prevent circumvention of access controls, broadly to works protected under Title 17, i.e., copyrighted works.

Second, as used in § 1201(a), to "circumvent a technological measure" means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). These two specific examples of unlawful circumvention under § 1201(a)—descrambling a scrambled work and decrypting an encrypted work—are acts that do not necessarily infringe or facilitate infringement of a copyright. Descrambling or decrypting only enables someone to watch or listen to a work without authorization, which is not necessarily an infringement of a copyright owner's traditional exclusive rights under § 106. Put differently, descrambling and decrypting do not necessarily result in someone's reproducing, distributing, publicly performing, or publicly displaying the copyrighted work, or creating derivative works based on the copyrighted work.

The third significant difference between the subsections is that § 1201(a)(1)(A) prohibits circumventing an effective access control measure, whereas § 1201(b) prohibits trafficking in circumventing devices, but does not prohibit circumvention itself because such conduct was already outlawed as copyright infringement. . . . This difference

reinforces our reading of § 1201(b) as strengthening copyright owners' traditional rights against copyright infringement and of § 1201(a) as granting copyright owners a new anti-circumvention right.

Fourth, in § 1201(a)(1)(B)–(D), Congress directs the Library of Congress ("Library") to identify classes of copyrighted works for which "noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the [anti-circumvention] prohibition contained in [§ 1201(a)(1)(A)] shall not apply to such users with respect to such classes of works for the ensuing 3-year period." There is no analogous provision in § 1201(b). We impute this lack of symmetry to Congress' need to balance copyright owners' new anti-circumvention right with the public's right to access the work. [T]he Library is only entitled to moderate the new anti-circumvention right created by, and hence subject to the limitations in, DMCA § 1201(a)(1).

Our reading of §§ 1201(a) and (b) ensures that neither section is rendered superfluous. A violation of § 1201(a)(1)(A), which prohibits circumvention itself, will not be a violation of § 1201(b), which does not contain an analogous prohibition on circumvention. A violation of § 1201(a)(2), which prohibits trafficking in devices that facilitate circumvention of *access* control measures, will not always be a violation of § 1201(b)(1), which prohibits trafficking in devices that facilitate circumvention of measures that protect against *copyright infringement*. Of course, if a copyright owner puts in place an effective measure that both (1) controls access and (2) protects against copyright infringement, a defendant who traffics in a device that circumvents that measure could be liable under both §§ 1201(a) and (b). Nonetheless, we read the differences in structure between §§ 1201(a) and (b) as reflecting Congress's intent to address distinct concerns by creating different rights with different elements.

3. Our construction of the DMCA is consistent with the legislative history

Although the text suffices to resolve the issues before us, we also consider the legislative history in order to address the parties' arguments concerning it. Our review of that history supports the view that Congress created a new anti-circumvention right in § 1201(a)(2) independent of traditional copyright infringement and granted copyright owners a new weapon against copyright infringement in § 1201(b)(1). For instance, the Senate Judiciary Committee report explains that §§ 1201(a)(2) and (b)(1) are "not interchangeable": they were "designed to protect two distinct rights and to target two distinct classes of devices," and "many devices will be subject to challenge only under one of the subsections." That is, § 1201(a)(2) "is designed to protect access to a copyrighted work," while § 1201(b)(1) "is designed to protect the traditional copyright rights of the copyright owner." Thus, the Senate Judiciary Committee understood § 1201 to create the following regime:

> [I]f an effective technological protection measure does nothing to prevent access to the plain text of the work, but is designed to prevent that work from being copied, then a potential cause of action against the manufacturer of a device designed to circumvent the measure lies under § 1201(b)(1), but not under § 1201(a)(2). Conversely, if an effective technological protection measure limits access to the plain text of a work only to those with authorized access, but provides no additional protection against copying, displaying, performing or distributing the work, then a potential cause of action against the manufacturer of a device designed to circumvent the measure lies under § 1201(a)(2), but not under § 1201(b).

The Senate Judiciary Committee proffered an example of § 1201(a) liability with no

nexus to infringement, stating that if an owner effectively protected access to a copyrighted work by use of a password, it would violate § 1201(a)(2)(A)

> [T]o defeat or bypass the password and to make the means to do so, as long as the primary purpose of the means was to perform this kind of act. This is roughly analogous to making it illegal to break into a house using a tool, the primary purpose of which is to break into houses.

The House Judiciary Committee similarly states of § 1201(a)(2), "The act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work is the electronic equivalent of breaking into a locked room in order to obtain a copy of a book." We note that bypassing a password and breaking into a locked room in order to read or view a copyrighted work would not infringe on any of the copyright owner's exclusive rights under § 106.

We read this legislative history as confirming Congress's intent, in light of the current digital age, to grant copyright owners an independent right to enforce the prohibition against circumvention of effective technological access controls. In § 1201(a), Congress was particularly concerned with encouraging copyright owners to make their works available in digital formats such as "on-demand" or "pay-per-view," which allow consumers effectively to "borrow" a copy of the work for a limited time or a limited number of uses. As the House Commerce Committee explained:

> [A]n increasing number of intellectual property works are being distributed using a "client-server" model, where the work is effectively "borrowed" by the user (e.g., infrequent users of expensive software purchase a certain number of uses, or viewers watch a movie on a pay-per-view basis). To operate in this environment, content providers will need both the technology to make new uses possible and the legal framework to ensure they can protect their work from piracy.

Our review of the legislative history supports our reading of § 1201: that section (a) creates a new anti-circumvention right distinct from copyright infringement, while section (b) strengthens the traditional prohibition against copyright infringement. We now review the decisions of the Federal Circuit that have interpreted § 1201 differently.

4. The Federal Circuit's decisions

The Federal Circuit has adopted a different approach to the DMCA. In essence, it requires § 1201(a) plaintiffs to demonstrate that the circumventing technology infringes or facilitates infringement of the plaintiff's copyright (an "infringement nexus requirement").

The seminal decision is *Chamberlain* (Fed. Cir. 2004). In *Chamberlain*, the plaintiff sold garage door openers ("GDOs") with a "rolling code" security system that purportedly reduced the risk of crime by constantly changing the transmitter signal necessary to open the door. Customers used the GDOs' transmitters to send the changing signal, which in turn opened or closed their garage doors.

Plaintiff sued the defendant, who sold "universal" GDO transmitters for use with plaintiff's GDOs, under § 1201(a)(2). The plaintiff alleged that its GDOs and transmitters both contained copyrighted computer programs and that its rolling code security system was a technological measure that controlled access to those programs. Accordingly, plaintiff alleged that the defendant—by selling GDO transmitters that were compatible with plaintiff's GDOs—had trafficked in a technology that was primarily used for the circumvention of a technological measure (the rolling code security system) that effectively controlled access to plaintiff's copyrighted works.

The Federal Circuit rejected the plaintiff's claim, holding that the defendant did not violate § 1201(a)(2) because, *inter alia*, the defendant's universal GDO transmitters

did not infringe or facilitate infringement of the plaintiff's copyrighted computer programs. The linchpin of the *Chamberlain* court's analysis is its conclusion that DMCA coverage is limited to a copyright owner's rights under the Copyright Act as set forth in § 106 of the Copyright Act. Thus, it held that § 1201(a) did not grant copyright owners a new anti-circumvention right, but instead, established new causes of action for a defendant's unauthorized access of copyrighted material when it infringes upon a copyright owner's rights under § 106. Accordingly, a § 1201(a)(2) plaintiff was required to demonstrate a nexus to infringement—i.e., that the defendant's trafficking in circumventing technology had a "reasonable relationship" to the protections that the Copyright Act affords copyright owners. The Federal Circuit explained:

> Defendants who traffic in devices that circumvent access controls in ways that facilitate infringement may be subject to liability under § 1201(a)(2). Defendants who use such devices may be subject to liability under § 1201(a)(1) whether they infringe or not. Because all defendants who traffic in devices that circumvent rights controls necessarily facilitate infringement, they may be subject to liability under § 1201(b). Defendants who use such devices may be subject to liability for copyright infringement. *And finally, defendants whose circumvention devices do not facilitate infringement are not subject to § 1201 liability.*

Chamberlain concluded that § 1201(a) created a new cause of action linked to copyright infringement, rather than a new anti-circumvention right separate from copyright infringement, for six reasons.

First, *Chamberlain* reasoned that Congress enacted the DMCA to balance the interests of copyright owners and information users, and an infringement nexus requirement was necessary to create an anti-circumvention right that truly achieved that balance. Second, *Chamberlain* feared that copyright owners could use an access control right to prohibit exclusively fair uses of their material even absent feared foul use. Third, *Chamberlain* feared that § 1201(a) would allow companies to leverage their sales into aftermarket monopolies, in potential violation of antitrust law and the doctrine of copyright misuse. Fourth, *Chamberlain* viewed an infringement nexus requirement as necessary to prevent "absurd and disastrous results," such as the existence of DMCA liability for disabling a burglary alarm to gain access to a home containing copyrighted materials.

Fifth, *Chamberlain* stated that an infringement nexus requirement might be necessary to render Congress's exercise of its Copyright Clause authority rational. The Copyright Clause gives Congress "the task of defining the scope of the limited monopoly that should be granted to authors . . . in order to give the public appropriate access to their work product." Without an infringement nexus requirement, Congress arguably would have allowed copyright owners in § 1201(a) to deny all access to the public by putting an effective access control measure in place that the public was not allowed to circumvent.

Finally, the *Chamberlain* court viewed an infringement nexus requirement as necessary for the Copyright Act to be internally consistent. It reasoned that § 1201(c)(1), enacted simultaneously, provides that "nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." The *Chamberlain* court opined that if § 1201(a) creates liability for access without regard to the remainder of the Copyright Act, it "would clearly affect rights and limitations, if not remedies and defenses."

Accordingly, the Federal Circuit held that a DMCA § 1201(a)(2) action was foreclosed to the extent that the defendant trafficked in a device that did not facilitate copyright infringement.

5. We decline to adopt an infringement nexus requirement

While we appreciate the policy considerations expressed by the Federal Circuit in Chamberlain, we are unable to follow its approach because it is contrary to the plain language of the statute. In addition, the Federal Circuit failed to recognize the rationale for the statutory construction that we have proffered. Also, its approach is based on policy concerns that are best directed to Congress in the first instance, or for which there appear to be other reasons that do not require such a convoluted construction of the statute's language.

i. Statutory inconsistencies

Were we to follow Chamberlain in imposing an infringement nexus requirement, we would have to disregard the plain language of the statute. Moreover, there is significant textual evidence showing Congress's intent to create a new anti-circumvention right in § 1201(a) distinct from infringement. As set forth *supra*, this evidence includes: (1) Congress's choice to link only § 1201(b)(1) explicitly to infringement; (2) Congress's provision in § 1201(a)(3)(A) that descrambling and decrypting devices can lead to § 1201(a) liability, even though descrambling and decrypting devices may only enable non-infringing access to a copyrighted work; and (3) Congress's creation of a mechanism in § 1201(a)(1)(B)–(D) to exempt certain non-infringing behavior from § 1201(a)(1) liability, a mechanism that would be unnecessary if an infringement nexus requirement existed. . . .

The Chamberlain court reasoned that if § 1201(a) creates liability for access without regard to the remainder of the Copyright Act, it "would clearly affect rights and limitations, if not remedies and defenses." This perceived tension is relieved by our recognition that § 1201(a) creates a new anti-circumvention right distinct from the traditional exclusive rights of a copyright owner. It follows that § 1201(a) does not limit the traditional framework of exclusive rights created by § 106, or defenses to those rights such as fair use.[12] We are thus unpersuaded by Chamberlain's reading of the DMCA's text and structure.

ii. Additional interpretive considerations

. . . Chamberlain relied heavily on policy considerations to support its reading of § 1201(a). . . . Chamberlain feared that § 1201(a) would allow companies to leverage their sales into aftermarket monopolies, in tension with antitrust law and the doctrine of copyright misuse. Concerning antitrust law, we note that there is no clear issue of anti-competitive behavior in this case because Blizzard does not seek to put a direct competitor who offers a competing role-playing game out of business and the parties have not argued this issue. If a § 1201(a)(2) defendant in a future case claims that a plaintiff is attempting to enforce its DMCA anti-circumvention right in a manner that violates antitrust law, we will then consider the interplay between this new anti-circumvention right and antitrust law.

Chamberlain also viewed an infringement nexus requirement as necessary to prevent "absurd and disastrous results," such as the existence of DMCA liability for disabling a burglary alarm to gain access to a home containing copyrighted materials. In addition, the Federal Circuit was concerned that, without an infringement nexus requirement, § 1201(a) would allow copyright owners to deny all access to the public by putting an effective access control measure in place that the public is not allowed to circumvent. Both concerns appear to be overstated, but even accepting them, arguendo, as legitimate concerns, they do not permit reading the statute as requiring the imposition

---

[12] Like the *Chamberlain* court, we need not and do not reach the relationship between fair use under § 107 of the Copyright Act and violations of § 1201. MDY has not claimed that Glider use is a "fair use" of WoW's dynamic non-literal elements. Accordingly, we too leave open the question whether fair use might serve as an affirmative defense to a *prima facie* violation of § 1201.

of an infringement nexus. As § 1201(a) creates a distinct right, it does not disturb the balance between public rights and the traditional rights of owners of copyright under the Copyright Act. Moreover, § 1201(a)(1)(B)–(D) allows the Library of Congress to create exceptions to the § 1201(a) anti-circumvention right in the public's interest. If greater protection of the public's ability to access copyrighted works is required, Congress can provide such protection by amending the statute.

In sum, we conclude that a fair reading of the statute (supported by legislative history) indicates that Congress created a distinct anti-circumvention right under § 1201(a) without an infringement nexus requirement. Thus, even accepting the validity of the concerns expressed in Chamberlain, those concerns do not authorize us to override congressional intent and add a non-textual element to the statute. Accordingly, we reject the imposition of an infringement nexus requirement. We now consider whether MDY has violated §§ 1201(a)(2) and (b)(1).

E. Blizzard's § 1201(a)(2) claim

1. WoW's literal elements and individual non-literal elements

We agree with the district court that MDY's Glider does not violate DMCA § 1201(a)(2) with respect to WoW's literal elements and individual non-literal elements, because Warden does not effectively control access to these WoW elements. First, Warden does not control access to WoW's literal elements because these elements—the game client's software code—are available on a player's hard drive once the game client software is installed. Second, as the district court found:

> [WoW's] individual nonliteral components may be accessed by a user without signing on to the server. As was demonstrated during trial, an owner of the game client software may use independently purchased computer programs to call up the visual images or the recorded sounds within the game client software. For instance, a user may call up and listen to the roar a particular monster makes within the game. Or the user may call up a virtual image of that monster.

Since a player need not encounter Warden to access WoW's individual non-literal elements, Warden does not effectively control access to those elements.

Our conclusion is in accord with the Sixth Circuit's decision in *Lexmark International v. Static Control Components* (6th Cir. 2004). In *Lexmark*, the plaintiff sold laser printers equipped with an authentication sequence, verified by the printer's copyrighted software, that ensured that only plaintiff's own toner cartridges could be inserted into the printers. The defendant sold microchips capable of generating an authentication sequence that rendered other manufacturers' cartridges compatible with plaintiff's printers.

The Sixth Circuit held that plaintiff's § 1201(a)(2) claim failed because its authentication sequence did not effectively control access to its copyrighted computer program. Rather, the mere purchase of one of plaintiff's printers allowed "access" to the copyrighted program. Any purchaser could read the program code directly from the printer memory without encountering the authentication sequence. The authentication sequence thus blocked only one form of access: the ability to make use of the printer. However, it left intact another form of access: the review and use of the computer program's literal code. The Sixth Circuit explained:

> Just as one would not say that a lock on the back door of a house "controls access" to a house whose front door does not contain a lock and just as one would not say that a lock on any door of a house "controls

> access" to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works. Add to this the fact that the DMCA not only requires the technological measure to "control access" but requires the measure to control that access "effectively," 17 U.S.C. § 1201(a)(2), and it seems clear that this provision does not naturally extend to a technological measure that restricts one form of access but leaves another route wide open.

Here, a player's purchase of the WoW game client allows access to the game's literal elements and individual non-literal elements. Warden blocks one form of access to these elements: the ability to access them while connected to a WoW server. However, analogously to the situation in *Lexmark*, Warden leaves open the ability to access these elements directly via the user's computer. We conclude that Warden is not an effective access control measure with respect to WoW's literal elements and individual non-literal elements, and therefore, that MDY does not violate § 1201(a)(2) with respect to these elements.

2. WoW's dynamic non-literal elements

We conclude that MDY meets each of the six textual elements for violating § 1201(a)(2) with respect to WoW's dynamic non-literal elements. That is, MDY (1) traffics in (2) a technology or part thereof (3) that is primarily designed, produced, or marketed for, or has limited commercially significant use other than (4) circumventing a technological measure (5) that effectively controls access (6) to a copyrighted work.

The first two elements are met because MDY "traffics in a technology or part thereof"—that is, it sells Glider. The third and fourth elements are met because Blizzard has established that MDY *markets* Glider for use in circumventing Warden, thus satisfying the requirement of § 1201(a)(2)(C).[16] . . . The sixth element is met because, as the district court held, WoW's dynamic non-literal elements constitute a copyrighted work.

The fifth element is met because Warden is an effective access control measure. To "effectively control access to a work," a technological measure must "in the ordinary course of its operation, require[ ] the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." Both of Warden's two components "require[ ] the application of information, or a process or a treatment . . . to gain access to the work." For a player to connect to Blizzard's servers which provide access to WoW's dynamic non-literal elements, scan.dll must scan the player's computer RAM and confirm the absence of any bots or cheats. The resident component also requires a "process" in order for the user to continue accessing the work: the user's computer must report portions of WoW code running in RAM to the server. Moreover, Warden's provisions were put into place by Blizzard, and thus, function "with

---

[16] To "circumvent a technological measure" under § 1201(a) means to "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, *without the authority of the copyright owner*." A circuit split exists with respect to the meaning of the phrase "without the authority of the copyright owner." The Federal Circuit has concluded that this definition imposes an additional requirement on a § 1201(a)(2) plaintiff: to show that the defendant's circumventing device enables third parties to access the copyrighted work without the copyright owner's authorization. *See Chamberlain*.The Second Circuit has adopted a different view, explaining that § 1201(a)(3)(A) plainly exempts from § 1201(a) liability those whom a copyright owner authorizes to circumvent an access control measure, not those whom a copyright owner authorizes to access the work. *Corley*. We find the Second Circuit's view to be the sounder construction . . . and conclude that § 1201(a)(2) does not require a plaintiff to show that the accused device enables third parties to access the work without the copyright owner's authorization. Thus, Blizzard has satisfied the "circumvention" element of a § 1201(a)(2) claim, because Blizzard has demonstrated that it did not authorize MDY to circumvent Warden.

the authority of the copyright owner." Accordingly, Warden effectively controls access to WoW's dynamic non-literal elements. We hold that MDY is liable under § 1201(a)(2) with respect to WoW's dynamic non-literal elements. . . .

F. Blizzard's § 1201(b)(1) claim

Blizzard may prevail under § 1201(b)(1) only if Warden "effectively protect[s] a right" of Blizzard under the Copyright Act. Blizzard contends that Warden protects its reproduction right against unauthorized copying. We disagree.

First, although WoW players copy the software code into RAM while playing the game, Blizzard's EULA and ToU authorize all licensed WoW players to do so. We have explained that ToU § 4(B)'s bot prohibition is a license covenant rather than a condition. Thus, a Glider user who violates this covenant does not infringe by continuing to copy code into RAM. Accordingly, MDY does not violate § 1201(b)(1) by enabling Glider users to avoid Warden's interruption of their *authorized* copying into RAM.

Second, although WoW players can theoretically record game play by taking screen shots, there is no evidence that Warden detects or prevents such allegedly infringing copying. This is logical, because Warden was designed to reduce the presence of cheats and bots, not to protect WoW's dynamic non-literal elements against copying. We conclude that Warden does not effectively protect any of Blizzard's rights under the Copyright Act, and MDY is not liable under § 1201(b)(1) for Glider's circumvention of Warden. . . .

VII.

. . . [W]e determine that MDY is not liable for secondary copyright infringement and is liable under the DMCA only for violation of § 1201(a)(2) with respect to WoW's dynamic non-literal elements. . . .

Questions:

1.) What is the significance of *MAI v. Peak*'s holding that RAM copies are "fixed" for purposes of copyright infringement to the *MDY* case? Put another way, if *MAI* were decided the other way, and RAM copies were too fleeting to infringe, how would this have changed the analysis in *MDY*?

2.) What is the difference between a covenant and condition? Why does it matter in this case?

3.) Have you ever read any Terms of Use agreements before clicking "I Agree"? Does it (should it) inform your analysis of *MDY* if you found that, in a related context, privacy scholars have estimated that an average user might access about 1450 websites per year that have privacy policies—note, not Terms of Use—and that it would take 244 hours a year to read those privacy policies?[1] It should be stressed that many other digital encounters—including those with games, phones and so on—*also* require assent to terms of use that are not captured in the study of *websites*. On the other hand, one does not have to assent to privacy policies to use many websites but at least formal assent to Terms of Use is necessary to use many services.

4.) "Were we to hold otherwise, Blizzard—or any software copyright holder—could designate any disfavored conduct during software use as copyright infringement, by

---

[1] Aleecia MacDonald & Lorrie Cantor, The Cost of Reading Privacy Policies http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

purporting to condition the license on the player's abstention from the disfavored conduct. . . . This would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners." Focus on the court's analysis of whether a violation of the Terms of Use is a condition or a covenant. The court rejects the formalistic argument suggested by *MAI* and § 106 that the code has been *copied* into RAM under an agreement and therefore that *any* violation of that agreement is a violation of copyright law. Instead, it focuses only on those violations of the TOU that have a nexus to the traditional rights of the copyright holder. Now compare this reasoning to the court's analysis of whether the copyright owner can impose through *digital* fences and watchdogs, requirements unrelated to copyright's traditional rights, and then label any attempt to get around them a violation of § 1201. **Why impose a "nexus to copyright infringement" requirement in one setting and then reject it for the other?** Why permit "rights-creep" by *code*, but not by *contract*? Is Judge Callahan a legal realist when it comes to § 106 but a formalist when it comes to § 1201? Is there some other explanation?

5.) This book is under a Creative Commons Attribution, Non Commercial, Sharealike license. You can find the license here. https://creativecommons.org/licenses/by-nc-sa/3.0/us/ You should look at the full terms of the license, available from that link, but the license deed (a human–friendly summary) is as follows:

You are free to:

Share — copy and redistribute the material in any medium or format

Adapt — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give **appropriate credit**, provide a link to the license, and **indicate if changes were made**. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NonCommercial — You may not use the material for **commercial purposes**.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the **same license** as the original.

No additional restrictions — You may not apply legal terms or **technological measures** that legally restrict others from doing anything the license permits.

Your use of this book is subject to the terms of the license. You can copy it, send copies by email, put it on your website, adapt it for your own course by cutting and editing it. But you must comply with the listed terms. Use the analysis supplied in *MDY*. Are these conditions? Covenants? Answer the following questions.

a.) Joe is a law student who wants to go into business for himself. He finds the digital

version of this book before his classmates realize they can download it freely. Joe offers to sell them digital versions for $10 each. Later, on Spring break, Joe's friends have their electronics stolen. Fearing professorial wrath, they are frantic to do their Intellectual Property reading. Joe has the only remaining iPad and he has a copy of the original pdf of this book on it. Ever the entrepreneur, Joe offers to let them read it on his device: $1 a minute.

b.) Joan is a professor who wants to impress her Dean with her productivity. She prints out a copy of the book, but simply removes the title page and replaces it with one naming her as the author.

c.) Jonathan, another professor, likes the book – except all the stuff about "framing" and "baselines." He removes that chapter and adds some of his own material, including a chapter on patent law's doctrine of equivalents. Jonathan really likes his version and does not want people meddling with it. He posts it on his own website for free download, but he uses the in-built restrictions in Microsoft Word to "freeze" the document. Editing is disabled.

d.) Jeremy gets an advance copy of the book and includes a lengthy review of the book in his Kindle Single "What's Wrong With Law Schools!" – a small ebook that he sells for $1.99. Jeremy is harshly critical of the book's approach and illustrates it with many quotations.

Have Joe, Joan, Jonathan or Jeremy violated the license? Exactly how? Be precise about the rights involved and the ways they were violated. Condition or covenant? What are the consequences if they have? Boyle and Jenkins get a lucrative offer from Aspen to sell the book commercially and decide to give up "all the hippy dippy open courseware stuff." They start sending DMCA takedown notices to anyone who posts a copy of the book. Sound? Are Boyle and Jenkins allowed to post a DRM-limited version of the book? (Think about this one carefully. Are they subject to the license?)

6.) Compare *MDY*'s and *Skylink*'s analyses of the reach of section 1201—which is more faithful to the language of the statute and the legislative history? What about the relevant policy arguments?

7.) "[I]n our view, an access control measure can both (1) attempt to block initial access and (2) revoke access if a secondary check determines that access was unauthorized." Should the court find a violation of a "technological measure" under 1201 only in circumvention of one that controls initial access to a work, or circumvention of any measure that can interfere with access after it has been lawfully gained? What are the implications of extending 1201(a) to the latter? Could Microsoft, for example, terminate Word if it finds you have a competing word processor on your laptop, or Apple shut down your phone if you have any disfavored app on it, and then label it a violation of Federal law were you to resist? Or does the language "if *access* was unauthorized" constrain the reach of this holding adequately? Is violation of the Terms of Use *as you are using your phone* enough to make your "access" "unauthorized"?

8.) What does *MDY* decide about the relationship of fair use to 1201? What does *Skylink* decide on the same issue? *Corley*? One court has ruled on this issue and two have declined to reach it. If they had to, what would they say?

PROBLEM 15-2

Google has decided to expand its search offerings to the "code" of that most powerful operating system of all, US law. Their lead engineer, John "Call me Von" Neumann has announced that researching Federal Law "should be as easy as Googling" and Google has initiated a secret project called Malomar to achieve this goal. Malomar attempts to replicate the success of the Google Books project, but to do so with Federal cases and statutes. Google has determined that it would be "inefficient" simply to scan all of those materials from paper books. Instead, it purchased a high level subscription to Westlaw and started a program of downloading all of the Federal cases and statutes through that service. The Malomar program logs onto Westlaw, downloads the cases, removes West's proprietary head notes and Key Numbers—all without a human being ever seeing the document.

Malomar was proceeding brilliantly until it hit a snag. Google had exceeded the maximum allowable number of downloads from its Westlaw account, which was terminated as a result. Foreseeing an endless game of cat and mouse, Neumann took a different approach. Westlaw offers access in two ways, through a simple browser interface and through a customized "client" program that resides on the user's computer and offers more features. Neumann had his software engineers decompile the Westlaw client software he had received with Google's first authorized account. (To get this account, he had to click "assent" to the Westlaw License. Had he read it, he would have found that the license forbids in its Terms of Service, *inter alia*, decompiling the licensed copy of the Westlaw client, exceeding download limits, falsifying passwords or usernames, and extracting material from the Westlaw database in order to compete commercially with West.) From this decompiled software he was able to deduce the mathematical characteristics of the usernames and passwords generated by the Westlaw system—the underlying equation that generates a pattern of letters and numbers making up an authorized username and password. While these were not in fact authorized accounts, the Westlaw system would recognize them as valid. Neumann kept meticulous records of each "account" used and every month sent Westlaw a check for the amount he would have been charged for a valid account.

Having "cracked the code" of the client software, Neumann had no further use for it. Instead, the Malomar program would log on as a newly created "user" through the browser interface, download a large number of cases and statutes—automatically redacting them as described earlier. Malomar downloads no materials other than Federal cases and statutes (all public domain material under § 105). It then repeats the process with a different username and password, all without human intervention at any point. Westlaw does have an online system that terminates the sessions of users who exceed download limits, but since Malomar constantly changes identities it is not affected by that system.

What is the potential liability of Neumann himself, and of the Malomar program, under DMCA 1201? What are the technological measures in play? Refer back to the specific statutory provisions and definitions, as well as the analysis in the three cases that you have read in this chapter. Does it matter that Malomar is ultimately only downloading public domain material? What about its removal of headnotes and Key Numbers? Does the possible breach of the Westlaw License also constitute copyright infringement?