IX. Technological Protections for Copyrighted Works

In this chapter, you will learn about the provisions of the Digital Millennium Copyright Act, codified in the Copyright Act principally in § 1201, that prohibit certain "circumventions" of technological protection measures that copyright owners may employ to control access to or use of copyrighted works. The § 1201 anti-circumvention provisions are one of the two primary changes to copyright law put into place by the Digital Millennium Copyright Act of 1998. The other is the § 512 safe-harbor provisions, which you studied in Chapter VII.

A. Early History of Technological Protection Measures

Since at least the early 1980s, some owners of copyrighted content have sought to supplement the rights that copyright provides with **technological protections**—technologies that work to prevent unauthorized access to, or copying of, copyrighted works. One early example was Macrovision, a technology introduced in the mid-1980s and deployed by the motion picture industry to prevent the unauthorized reproduction of pre-recorded videocassettes. Devices were quickly introduced that worked to defeat Macrovision, but these devices never gained widespread distribution, possibly because the incentive to pirate pre-recorded videotapes was blunted by the wide availability of cheap video rentals as well as home taping using the consumer-oriented video cassette recorders (VCRs) that became popular around the same time that Macrovision was introduced. As you read in Chapter VI, the Supreme Court's opinion in *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), held that VCR taping for the purposes of time shifting constituted fair use.

Also in the 1980s, satellite and cable television broadcasters introduced various forms of encryption to prevent unauthorized access to their services. However, these early cable and satellite technological protections were far from foolproof, and technologies and devices to defeat them were made widely available soon after their introduction. Congress legislated to prohibit unauthorized satellite and cable "black box" decoders, Pub. L. No. 100-667, § 204, 102 Stat. 3935 (codified as amended at 47 U.S.C. § 605(e)(4) (1988)); that law helped limit the availability of the black box devices, though it never succeeded in driving them out of the market entirely.

The most heated battle over technological protections in the 1980s played out in the software industry. Concerned with widespread unauthorized reproduction of their copyrighted programs, software companies began to experiment with a variety of technologies aimed at limiting access and the ability to copy. Some of these technologies frustrated legitimate users, who experienced problems running the programs they'd paid for and even, on occasion, computer crashes. And almost as quickly as software companies introduced new technological protections, hackers developed ways to defeat them. By the early 1990s, the software industry had significantly reduced its reliance on copy-protection technologies. On the other hand, simple access-protection technologies, such as access codes, remained in widespread use.

B. The Audio Home Recording Act

The use of technological protections took an important turn with the introduction, first in Japan and then in the United States, of the digital audiotape (DAT) recording format—the first widely-distributed digital copying technology. After prolonged negotiations, the consumer electronics companies and music and recording industry firms involved in the conception and rollout of DAT coordinated on a technical protocol for DAT copy protection—the so-called Serial Copy Management System (SCMS)—and agreed to include SCMS in all consumer DAT recorders. SCMS allowed the making of first-generation copies (copies made from source material) at the same fidelity as the source material, but blocked subsequent-generation or "serial" copies (copies made from copies).

The firms behind SCMS also sought to have their favored technological protection measure adopted and enforced by law. In 1992, Congress acceded to this desire, passing the Audio Home Recording Act (AHRA), which you first encountered in your study of the music industry in Chapter V. The AHRA requires that all "digital audio recording devices" incorporate SCMS, and it bans the manufacture or distribution of any device or the provision of any service that would circumvent SCMS. 17 U.S.C. § 1002. Note that the statute's definition of "digital audio recording device" limits the AHRA's coverage to devices that are specifically marketed as digital audio recording devices, such as CD-R recorders when marketed as standalone devices. It does not cover general-purpose computers, even though they are often used to copy digital audio files:

> *A "digital audio recording device" is any machine or device of a type commonly distributed to individuals for use by individuals, whether or not included with or as part of some other machine or device, the digital recording function of which is designed or marketed for the primary purpose of, and that is capable of, making a digital audio copied recording for private use.*

Id. § 1001(3). Thus, the boundary between what is and is not covered by the AHRA is determined by whether or not a particular device is marketed or designed to make audio recordings, not the device's capabilities. An iPhone or Android phone that includes a capability to copy digital audio files is not a "digital audio recording device" under the AHRA, because those devices are not marketed primarily for making copies of music.

Further—as you read in Chapter V—the AHRA requires manufacturers of digital audio recording devices for the consumer market to pay royalties on digital audio recording media and equipment marketed to consumers (as opposed to professionals). Royalties collected under the AHRA scheme are pooled and then divided among copyright owners of sound recordings and musical compositions, as well as featured recording artists, with a small percentage paid to non-featured musicians and vocalists. *Id.* §§ 1003-1007. The AHRA bars infringement actions against consumers for personal, noncommercial copying using covered media, and similarly bars actions against manufacturers and distributors of covered digital audio recording devices and media. *Id.* § 1008.

The AHRA's scheme of mandated technical protections against serial copying—a statutory levy that is applied to copying equipment and media, the division of pooled royalties among copyright owners and other market participants, and immunity from suit for use of covered technology—was a unique approach to the copyright issues raised by digital copying technologies. The approach has, however, largely been superseded by technological developments. Most audio (and other) copying these days is undertaken using general-purpose computers and other devices, such as smartphones, rather than the specialized devices covered by the AHRA.

C. The Digital Millennium Copyright Act

Although the rapid technological progression from specialized digital recording devices to the use of general-purpose computers to reproduce, distribute, and modify digital files made the AHRA largely obsolete, content owners remained interested in bolstering federal law with provisions that reinforce technological protections by banning the use or distribution of technologies aimed at circumventing these protections. But opposition from technology companies, librarians, consumer groups, and others was sufficient to counter the push to provide legal anti-circumvention protection. The stalemate was broken in 1996 at the international conference held to draft the World Intellectual Property Organization Copyright Treaty. Representatives at that proceeding agreed to a provision, adopted as Article 11 of the treaty, that mandates the adoption of legal protections against the circumvention of technological protection measures:

> *Contracting Parties shall 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.*

Their hand strengthened by the treaty mandate, supporters of anti-circumvention protections prevailed in a renewed U.S. lobbying campaign, and the protections were enacted as part of the Digital Millennium Copyright Act of 1998 (DMCA). The DMCA's anti-circumvention provisions were codified principally in 17 U.S.C. § 1201.

1. Section 1201

There are two key distinctions that drive the structure of § 1201. First, § 1201 distinguishes between technologies that control *access* to a copyrighted work and those that control *rights*—that is, technologies that "effectively protect the right of a copyright owner." Second, § 1201 distinguishes between *individual acts of circumvention* and the *distribution of technologies designed to aid in circumvention.*

These two distinctions are reflected in the particular subparts of § 1201, which can be summarized as follows:

1) § 1201(a)(1) prohibits *individual acts* of circumvention of *access controls*;
2) § 1201(a)(2) prohibits *distribution* of technologies designed to aid in circumvention of *access controls*;
3) § 1201(b) prohibits *distribution* of technologies designed to aid in circumvention of *rights controls*; and
4) nothing in § 1201 prohibits *individual acts of* circumvention of *rights controls*.

Violations of § 1201 do not constitute copyright infringement. Rather, they are violations of the DMCA. Section 1203 sets out the civil remedies that provided under the DMCA, and § 1204 does the same for the criminal remedies that the DMCA provides.

Why do you think that copyright holders find it useful to have legal protection against circumvention of their access or rights controls? What might happen without such legal protection? Does the addition of § 1201 raise any worries about upsetting the internal balances of copyright law or of harms to the public that might arise from providing anti-circumvention protections? In particular, what if a member of the public wants to engage in a fair use of a work that is protected by an access control? By a rights control? Note in particular that because § 1201 leaves unregulated individual circumvention of rights controls, an individual who has lawful access to a work is free to circumvent rights controls to make a use permitted by fair use. That same freedom, as we shall see, does not apply to circumvention of *access controls* for the purpose of making a fair use.

2. Section 1201 Triennial Review

Section 1201(a)(1) also includes what Congress characterized as a "fail-safe" mechanism: a triennial review. This review requires the Librarian of Congress, following a rulemaking proceeding held every three years, to exempt from the DMCA's prohibition on circumvention any class of copyrighted works as to which the Librarian has determined that non-infringing uses are, or are likely to be, adversely affected by circumvention prohibition in the succeeding three-year period. The Librarian's determination to grant an exemption is based upon the recommendation of the Register of Copyrights, who conducts the rulemaking proceeding. The Register, in turn, consults with the Assistant Secretary for Communications and Information of the Department of Commerce, who oversees the National Telecommunications and Information Administration. Recently, the D.C. Circuit held that the Copyright Office's statutory authority here is subject to judicial review under the standards set forth in the Administrative Procedure Act. Med. Imaging & Tech. All. v. Library of Cong., --- F.4th ---- (D.C. Cir. 2024).

The primary responsibility of the Register and the Librarian in the rulemaking proceeding is to assess whether the implementation of *access controls* within the meaning of § 1201(a)(1) impairs the ability of individuals to make non-infringing uses of copyrighted works. Significantly, the exemptions do not apply to other parts of

§ 1201. Most notably, exemptions do not apply to § 1201(a)(2), which bars trafficking in products and services used to circumvent access controls, or § 1201(b), which bars trafficking in products and services used to circumvent rights controls. Why do you think that exemptions apply only to access controls? And why do you think they apply only to individual uses of circumvention technologies, and not "trafficking" of those technologies by others?

In considering exemptions, the Register develops a comprehensive administrative record using information submitted by interested members of the public and makes recommendations to the Librarian concerning whether exemptions are warranted based on that record. Under the statutory framework, the Librarian, and thus the Register, must consider "(i) the availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and (v) such other factors as the Librarian considers appropriate." 17 U.S.C. § 1201(a)(1)(C).

The most recent triennial review was conducted in 2021, and a new 2024 triennial review is underway as of the time of this writing. In the 2021 review, the Library of Congress broadened a variety of exemptions for the diagnosis, maintenance, and repair of consumer devices that rely on software to function, and expanded the categories of people able to take advantage of a previously-granted exemption for reproducing clips of audiovisual works for educational use. The Library also renewed other important exemptions that had previously been granted. For a complete list of exemptions, see https://www.govinfo.gov/content/pkg/FR-2021-10-28/pdf/2021-23311.pdf.

As you read the next case, think about whether the court has provided an adequate account of its characterization of the technological protection at issue as an access control. Think about whether the characterization of the technological protection as controlling access rather than protecting a copyright owner's rights makes a difference to the outcome of the case.

Universal City Studios, Inc. v. Reimerdes

111 F. Supp. 2d 294 (S.D.N.Y. 2000)

KAPLAN, J.:

[1] Plaintiffs, eight major United States motion picture studios, distribute many of their copyrighted motion pictures for home use on digital versatile disks ("DVDs"), which contain copies of the motion pictures in digital form. They protect those motion pictures from copying by using an encryption system called CSS. CSS-protected motion pictures on DVDs may be viewed only on players and computer drives equipped with licensed technology that permits the devices to decrypt and play—but not to copy—the films.

[2] Late last year, computer hackers devised a computer program called DeCSS that circumvents the CSS protection system and allows CSS-protected motion pictures to be copied and played on devices that lack the licensed decryption technology. Defendants quickly posted DeCSS on their Internet web site, thus making it readily available to much of the world. Plaintiffs promptly brought this action under the Digital Millennium Copyright Act to enjoin defendants from posting DeCSS and to prevent them from electronically "linking" their site to others that post DeCSS. Defendants responded with what they termed "electronic civil disobedience"—increasing their efforts to link their web site to a large number of others that continue to make DeCSS available.

[3] Defendants contend that their actions do not violate the DMCA and, in any case, that the DMCA, as applied to computer programs, or code, violates the First Amendment....

[4] CSS, or Content Scramble System, is an access control and copy prevention system for DVDs developed by the motion picture companies, including plaintiffs. It is an encryption-based system that requires the use of appropriately configured hardware such as a DVD player or a computer DVD drive to decrypt, unscramble and play back, but not copy, motion pictures on DVDs. The technology necessary to configure DVD players and drives to play CSS-protected DVDs has been licensed to hundreds of manufacturers in the United States and around the world.

[5] DeCSS is a software utility, or computer program, that enables users to break the CSS copy protection system and hence to view DVDs on unlicensed players and make digital copies of DVD movies. The quality of motion pictures decrypted by DeCSS is virtually identical to that of encrypted movies on DVD....

[6] Plaintiffs are eight major motion picture studios....

[7] Defendant Eric Corley is viewed as a leader of the computer hacker community and goes by the name Emmanuel Goldstein, after the leader of the underground in George Orwell's classic, *1984*.... In addition, defendants operate a web site located at <http://www.2600.com> ....

[8] Prior to January 2000, when this action was commenced, defendants posted the source and object code for DeCSS on the 2600.com web site, from which they could be downloaded easily. At that time, 2600.com contained also a list of links to other web sites purporting to post DeCSS....

[9] The major motion picture studios typically distribute films in a sequence of so-called windows, each window referring to a separate channel of distribution and thus to a separate source of revenue. The first window generally is theatrical release, distribution, and exhibition. Subsequently, films are distributed to airlines and hotels, then to the home market, then to pay television, cable and, eventually, free television broadcast. The home market is important to plaintiffs, as it represents a significant source of revenue.

[10] Motion pictures first were, and still are, distributed to the home market in the form of video cassette tapes. In the early 1990's, however, the major movie studios began to explore distribution to the home market in digital format, which offered substantially higher audio and visual quality and greater longevity than video cassette tapes. This technology, which in 1995 became what is known today as DVD, brought with it a new problem—increased risk of piracy by virtue of the fact that digital files, unlike the material on video cassettes, can be copied without degradation from generation to generation....

[11] Discussions among the studios with the goal of organizing a unified response to the piracy threat began in earnest in late 1995 or early 1996.... In 1996, Matsushita Electric Industrial Co. and Toshiba Corp., presented—and the studios adopted—CSS....

[12] CSS involves encrypting, according to an encryption algorithm, the digital sound and graphics files on a DVD that together constitute a motion picture. A CSS-protected DVD can be decrypted by an appropriate decryption algorithm that employs a series of keys stored on the DVD and the DVD player. In consequence, only players and drives containing the appropriate keys are able to decrypt DVD files and thereby play movies stored on DVDs.

[13] As the motion picture companies did not themselves develop CSS and, in any case, are not in the business of making DVD players and drives, the technology for making compliant devices, i.e., devices with CSS keys, had to be licensed to consumer electronics manufacturers. In order to ensure that the decryption technology did not become generally available and that compliant devices could not be used to copy as well as merely to

play CSS-protected movies, the technology is licensed subject to strict security requirements. Moreover, manufacturers may not, consistent with their licenses, make equipment that would supply digital output that could be used in copying protected DVDs….

[14] With CSS in place, the studios introduced DVDs on the consumer market in early 1997. All or most of the motion pictures released on DVD were, and continue to be, encrypted with CSS technology….

[15] In late September 1999, Jon Johansen, a Norwegian subject then fifteen years of age, and two individuals he "met" under pseudonyms over the Internet, reverse engineered a licensed DVD player and discovered the CSS encryption algorithm and keys. They used this information to create DeCSS, a program capable of decrypting or "ripping" encrypted DVDs, thereby allowing playback on non-compliant computers as well as the copying of decrypted files to computer hard drives. Mr. Johansen then posted the executable code on his personal Internet web site and informed members of an Internet mailing list that he had done so. Neither Mr. Johansen nor his collaborators obtained a license from the DVD [Copy Control Association administering CSS].

[16] Although Mr. Johansen testified at trial that he created DeCSS in order to make a DVD player that would operate on a computer running the Linux operating system, DeCSS is a Windows executable file; that is, it can be executed only on computers running the Windows operating system. Mr. Johansen explained the fact that he created a Windows rather than a Linux program by asserting that Linux, at the time he created DeCSS, did not support the file system used on DVDs. Hence, it was necessary, he said, to decrypt the DVD on a Windows computer in order subsequently to play the decrypted files on a Linux machine. Assuming that to be true, however, the fact remains that Mr. Johansen created DeCSS in the full knowledge that it could be used on computers running Windows rather than Linux. Moreover, he was well aware that the files, once decrypted, could be copied like any other computer files….

[17] In November 1999, defendants' web site began to offer DeCSS for download. It established also a list of links to several web sites that purportedly "mirrored" or offered DeCSS for download. The links on defendants' mirror list fall into one of three categories. By clicking the mouse on one of these links, the user may be brought to a page on the linked-to site on which there appears a further link to the DeCSS software. If the user then clicks on the DeCSS link, download of the software begins. This page may or may not contain content other than the DeCSS link. Alternatively, the user may be brought to a page on the linked-to site that does not itself purport to link to DeCSS, but that links, either directly or via a series of other pages on the site, to another page on the site on which there appears a link to the DeCSS software. Finally, the user may be brought directly to the DeCSS link on the linked-to site such that download of DeCSS begins immediately without further user intervention….

[18] …. In January 2000, the studios filed this lawsuit against defendant Eric Corley and two others….

[19] Following the issuance of [a] preliminary injunction, defendants removed DeCSS from the 2600.com web site. In what they termed an act of "electronic civil disobedience," however, they continued to support links to other web sites purporting to offer DeCSS for download, a list which had grown to nearly five hundred by July 2000….

[20] …. [T]he availability of DeCSS on the Internet effectively has compromised plaintiffs' system of copyright protection for DVDs, requiring them either to tolerate increased piracy or to expend resources to develop and implement a replacement system unless the availability of DeCSS is terminated. It is analogous to the publication of a bank vault combination in a national newspaper. Even if no one uses the combination to open the vault, its mere publication has the effect of defeating the bank's security system, forcing the bank to reprogram the lock. Development and implementation of a new DVD copy protection system, however, is far more difficult and costly than reprogramming a combination lock and may carry with it the added problem of

rendering the existing installed base of compliant DVD players obsolete….

II. The Digital Millennium Copyright Act …

[21] The DMCA contains two principal anticircumvention provisions. The first, Section 1201(a)(1), governs "[t]he act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work," an act described by Congress as "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book." The second, Section 1201(a)(2), which is the focus of this case, "supplements the prohibition against the act of circumvention in paragraph (a)(1) with prohibitions on creating and making available certain technologies … developed or advertised to defeat technological protections against unauthorized access to a work." As defendants are accused here only of posting and linking to other sites posting DeCSS, and not of using it themselves to bypass plaintiffs' access controls, it is principally the second of the anticircumvention provisions that is at issue in this case.

B. Posting of DeCSS

1. Violation of Anti–Trafficking Provision

[22] Section 1201(a)(2) of the Copyright Act, part of the DMCA, provides that:

> *No person shall … offer to the public, provide or otherwise traffic in any technology … that—*
>
> > *(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act];*
> > *(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 [the Copyright Act]; 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 [the Copyright Act]."*

[23] In this case, defendants concededly offered and provided and, absent a court order, would continue to offer and provide DeCSS to the public by making it available for download on the 2600.com web site. DeCSS, a computer program, unquestionably is "technology" within the meaning of the statute. "[C]ircumvent a technological measure" is defined to mean descrambling a scrambled work, decrypting 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), so DeCSS clearly is a means of circumventing a technological access control measure.[137] In consequence, if CSS otherwise falls within paragraphs (A), (B) or (C) of Section

[137] Decryption or avoidance of an access control measure is not "circumvention" within the meaning of the statute unless it occurs "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). Defendants posit that purchasers of a DVD acquire the right "to perform all acts with it that are not exclusively granted to the copyright holder." Based on this premise, they argue that DeCSS does not circumvent CSS within the meaning of the statute because the Copyright Act does not grant the copyright holder the right to prohibit purchasers from decrypting. As the copyright holder has no statutory right to prohibit decryption, the argument goes, decryption cannot be understood as unlawful circumvention. The argument is pure sophistry. The DMCA proscribes trafficking in technology that decrypts or avoids an access control measure without the copyright holder consenting to the decryption or avoidance. Defendants' argument seems to be a corruption of the first sale doctrine, which holds that the copyright holder, notwithstanding the exclusive distribution right conferred by Section 106(3) of the Copyright Act is deemed by its "first sale" of a copy of the copyrighted work to have consented to subsequent sale of the copy.

1201(a)(2), and if none of the statutory exceptions applies to their actions, defendants have violated and, unless enjoined, will continue to violate the DMCA by posting DeCSS.

a. Section 1201(a)(2)(A) …

[24] During pretrial proceedings and at trial, defendants attacked plaintiffs' Section 1201(a)(2)(A) claim, arguing that CSS, which is based on a 40-bit encryption key, is a weak cipher that does not "effectively control" access to plaintiffs' copyrighted works.... [T]he contention is indefensible as a matter of law.

[25] First, the statute expressly provides that "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 a work." 17 U.S.C. § 1201(a)(3)(B). One cannot gain access to a CSS-protected work on a DVD without application of the three keys that are required by the software. One cannot lawfully gain access to the keys except by entering into a license with the DVD [Copy Control Association] under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license. In consequence, under the express terms of the statute, CSS "effectively controls access" to copyrighted DVD movies. It does so, within the meaning of the statute, whether or not it is a strong means of protection....

[26] As CSS effectively controls access to plaintiffs' copyrighted works, the only remaining question under Section 1201(a)(2)(A) is whether DeCSS was designed primarily to circumvent CSS. The answer is perfectly obvious. By the admission of both Jon Johansen, the programmer who principally wrote DeCSS, and defendant Corley, DeCSS was created solely for the purpose of decrypting CSS—that is all it does. Hence, absent satisfaction of a statutory exception, defendants clearly violated Section 1201(a)(2)(A) by posting DeCSS to their web site....

[27] Perhaps the centerpiece of defendants' statutory position is the contention that DeCSS was not created for the purpose of pirating copyrighted motion pictures. Rather, they argue, it was written to further the development of a DVD player that would run under the Linux operating system, as there allegedly were no Linux compatible players on the market at the time....

[28] As the earlier discussion demonstrates, the question whether the development of a Linux DVD player motivated those who wrote DeCSS is immaterial to the question whether the defendants now before the Court violated the anti-trafficking provision of the DMCA. The inescapable facts are that (1) CSS is a technological means that effectively controls access to plaintiffs' copyrighted works, (2) the one and only function of DeCSS is to circumvent CSS, and (3) defendants offered and provided DeCSS by posting it on their web site. Whether defendants did so in order to infringe, or to permit or encourage others to infringe, copyrighted works in violation of other provisions of the Copyright Act simply does not matter for purposes of Section 1201(a)(2). The offering or provision of the program is the prohibited conduct—and it is prohibited irrespective of why the program was written, except to whatever extent motive may be germane to determining whether their conduct falls within one of the statutory exceptions.

2. Statutory Exceptions

[29] Earlier in the litigation, defendants contended that their activities came within several exceptions contained in the DMCA and the Copyright Act and constitute fair use under the Copyright Act. Their post-trial memorandum appears to confine their argument to the reverse engineering exception. In any case, all of their assertions are entirely without merit....

[30] Defendants claim to fall under Section 1201(f) of the statute, which provides in substance that one may circumvent, or develop and employ technological means to circumvent, access control measures in order to

achieve interoperability with another computer program provided that doing so does not infringe another's copyright and, in addition, that one may make information acquired through such efforts "available to others, if the person [in question] ... provides such information solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement...." They contend that DeCSS is necessary to achieve interoperability between computers running the Linux operating system and DVDs and that this exception therefore is satisfied. This contention fails.

[31] First, Section 1201(f)(3) permits information acquired through reverse engineering to be made available to others only by the person who acquired the information. But these defendants did not do any reverse engineering. They simply took DeCSS off someone else's web site and posted it on their own.

[32] Defendants would be in no stronger position even if they had authored DeCSS. The right to make the information available extends only to dissemination "solely for the purpose" of achieving interoperability as defined in the statute. It does not apply to public dissemination of means of circumvention, as the legislative history confirms. These defendants, however, did not post DeCSS "solely" to achieve interoperability with Linux or anything else.

[33] Finally, it is important to recognize that even the creators of DeCSS cannot credibly maintain that the "sole" purpose of DeCSS was to create a Linux DVD player. DeCSS concededly was developed on and runs under Windows—a far more widely used operating system. The developers of DeCSS therefore knew that DeCSS could be used to decrypt and play DVD movies on Windows as well as Linux machines. They knew also that the decrypted files could be copied like any other unprotected computer file. Moreover, the Court does not credit Mr. Johansen's testimony that he created DeCSS solely for the purpose of building a Linux player....

[34] Section 1201(g)(4) provides in relevant part that:

> *Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to—*
>
> > *(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and*
> > *(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).*

[35] Paragraph (2) in relevant part permits circumvention of technological measures in the course of good faith encryption research if:

> > *(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;*
> > *(B) such act is necessary to conduct such encryption research;*
> > *(C) the person made a good faith effort to obtain authorization before the circumvention; and*
> > *(D) such act does not constitute infringement under this title....*

[36] In determining whether one is engaged in good faith encryption research, the Court is instructed to consider factors including whether the results of the putative encryption research are disseminated in a manner designed to advance the state of knowledge of encryption technology versus facilitation of copyright

infringement, whether the person in question is engaged in legitimate study of or work in encryption, and whether the results of the research are communicated in a timely fashion to the copyright owner.

[37] Neither of the defendants remaining in this case was or is involved in good faith encryption research. They posted DeCSS for all the world to see. There is no evidence that they made any effort to provide the results of the DeCSS effort to the copyright owners. Surely there is no suggestion that either of them made a good faith effort to obtain authorization from the copyright owners. Accordingly, defendants are not protected by Section 1201(g)....

[38] Finally, defendants rely on the doctrine of fair use. Stated in its most general terms, the doctrine, now codified in Section 107 of the Copyright Act, limits the exclusive rights of a copyright holder by permitting others to make limited use of portions of the copyrighted work, for appropriate purposes, free of liability for copyright infringement. For example, it is permissible for one other than the copyright owner to reprint or quote a suitable part of a copyrighted book or article in certain circumstances. The doctrine traditionally has facilitated literary and artistic criticism, teaching and scholarship, and other socially useful forms of expression. It has been viewed by courts as a safety valve that accommodates the exclusive rights conferred by copyright with the freedom of expression guaranteed by the First Amendment.

[39] The use of technological means of controlling access to a copyrighted work may affect the ability to make fair uses of the work. Focusing specifically on the facts of this case, the application of CSS to encrypt a copyrighted motion picture requires the use of a compliant DVD player to view or listen to the movie. Perhaps more significantly, it prevents exact copying of either the video or the audio portion of all or any part of the film. This latter point means that certain uses that might qualify as "fair" for purposes of copyright infringement—for example, the preparation by a film studies professor of a single CD-ROM or tape containing two scenes from different movies in order to illustrate a point in a lecture on cinematography, as opposed to showing relevant parts of two different DVDs—would be difficult or impossible absent circumvention of the CSS encryption. Defendants therefore argue that the DMCA cannot properly be construed to make it difficult or impossible to make any fair use of plaintiffs' copyrighted works and that the statute therefore does not reach their activities, which are simply a means to enable users of DeCSS to make such fair uses.

[40] Defendants have focused on a significant point. Access control measures such as CSS do involve some risk of preventing lawful as well as unlawful uses of copyrighted material. Congress, however, clearly faced up to and dealt with this question in enacting the DMCA.

[41] The Court begins its statutory analysis, as it must, with the language of the statute. Section 107 of the Copyright Act provides in critical part that certain uses of copyrighted works that otherwise would be wrongful are "not ... infringement[s] of copyright." Defendants, however, are not here sued for copyright infringement. They are sued for offering and providing technology designed to circumvent technological measures that control access to copyrighted works and otherwise violating Section 1201(a)(2) of the Act. If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate.

[42] Congress was well aware during the consideration of the DMCA of the traditional role of the fair use defense in accommodating the exclusive rights of copyright owners with the legitimate interests of noninfringing users of portions of copyrighted works. It recognized the contention, voiced by a range of constituencies concerned with the legislation, that technological controls on access to copyrighted works might erode fair use by preventing access even for uses that would be deemed "fair" if only access might be gained. And it struck a balance among the competing interests.

[43] The first element of the balance was the careful limitation of Section 1201(a)(1)'s prohibition of the act of circumvention to the act itself so as not to apply to subsequent actions of a person once he or she has obtained authorized access to a copy of a [copyrighted] work. By doing so, it left the traditional defenses to copyright infringement, including fair use, fully applicable provided the access is authorized.

[44] Second, Congress delayed the effective date of Section 1201(a)(1)'s prohibition of the act of circumvention for two years pending further investigation about how best to reconcile Section 1201(a)(1) with fair use concerns. Following that investigation, which is being carried out in the form of a rule-making by the Register of Copyright, the prohibition will not apply to users of particular classes of copyrighted works who demonstrate that their ability to make noninfringing uses of those classes of works would be affected adversely by Section 1201(a)(1).

[45] Third, it created a series of exceptions to aspects of Section 1201(a) for certain uses that Congress thought "fair," including reverse engineering, security testing, good faith encryption research, and certain uses by nonprofit libraries, archives and educational institutions.

[46] Defendants claim also that the possibility that DeCSS might be used for the purpose of gaining access to copyrighted works in order to make fair use of those works saves them under *Sony Corp. v. Universal City Studios, Inc.* But they are mistaken. *Sony* does not apply to the activities with which defendants here are charged. Even if it did, it would not govern here....

[47] When *Sony* was decided, the only question was whether the manufacturers could be held liable for infringement by those who purchased equipment from them in circumstances in which there were many noninfringing uses for their equipment. But that is not the question now before this Court. The question here is whether the possibility of noninfringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by the defendants saves the defendants from liability under Section 1201. But nothing in Section 1201 so suggests. By prohibiting the provision of circumvention technology, the DMCA fundamentally altered the landscape. A given device or piece of technology might have a substantial noninfringing use, and hence be immune from attack under *Sony*'s construction of the Copyright Act—but nonetheless still be subject to suppression under Section 1201. Indeed, Congress explicitly noted that Section 1201 does not incorporate *Sony.*

[48] The policy concerns raised by defendants were considered by Congress. Having considered them, Congress crafted a statute that, so far as the applicability of the fair use defense to Section 1201(a) claims is concerned, is crystal clear. In such circumstances, courts may not undo what Congress so plainly has done by "construing" the words of a statute to accomplish a result that Congress rejected. The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so is a matter for Congress unless Congress' decision contravenes the Constitution, a matter to which the Court turns below. Defendants' statutory fair use argument therefore is entirely without merit.

C. Linking to Sites Offering DeCSS

[49] Plaintiffs seek also to enjoin defendants from "linking" their 2600.com web site to other sites that make DeCSS available to users. ... The dispositive question is whether linking to another web site containing DeCSS constitutes "offer[ing DeCSS] to the public" or "provid[ing] or otherwise traffic[king]" in it within the meaning of the DMCA. Answering this question requires careful consideration of the nature and types of linking....

[50] To the extent that defendants have linked to sites that automatically commence the process of downloading DeCSS upon a user being transferred by defendants' hyperlinks, there can be no serious question. Defendants are engaged in the functional equivalent of transferring the DeCSS code to the user themselves.

[51] Substantially the same is true of defendants' hyperlinks to web pages that display nothing more than the DeCSS code or present the user only with the choice of commencing a download of DeCSS and no other content. The only distinction is that the entity extending to the user the option of downloading the program is the transferee site rather than defendants, a distinction without a difference.

[52] Potentially more troublesome might be links to pages that offer a good deal of content other than DeCSS but that offer a hyperlink for downloading, or transferring to a page for downloading, DeCSS. If one assumed, for the purposes of argument, that the *Los Angeles Times* web site somewhere contained the DeCSS code, it would be wrong to say that anyone who linked to the *Los Angeles Times* web site, regardless of purpose or the manner in which the link was described, thereby offered, provided or otherwise trafficked in DeCSS merely because DeCSS happened to be available on a site to which one linked. But that is not this case. Defendants urged others to post DeCSS in an effort to disseminate DeCSS and to inform defendants that they were doing so. Defendants then linked their site to those "mirror" sites, after first checking to ensure that the mirror sites in fact were posting DeCSS or something that looked like it, and proclaimed on their own site that DeCSS could be had by clicking on the hyperlinks on defendants' site. By doing so, they offered, provided or otherwise trafficked in DeCSS, and they continue to do so to this day….

[53] Defendants argue that the DMCA, at least as applied to prevent the public dissemination of DeCSS, violates the First Amendment to the Constitution. They claim that it does so in two ways. First, they argue that computer code is protected speech and that the DMCA's prohibition of dissemination of DeCSS therefore violates defendants' First Amendment rights. Second, they contend that the DMCA is unconstitutionally overbroad, chiefly because its prohibition of the dissemination of decryption technology prevents third parties from making fair use of plaintiffs' encrypted works, and vague. They argue also that a prohibition on their linking to sites that make DeCSS available is unconstitutional for much the same reasons….

[54] Defendants' assertion that computer code is "protected" by the First Amendment is quite understandable…. All modes of expression are covered by the First Amendment in the sense that the constitutionality of their regulation must be determined by reference to First Amendment doctrine and analysis. Regulation of different categories of expression, however, is subject to varying levels of judicial scrutiny. Thus, to say that a particular form of expression is "protected" by the First Amendment means that the constitutionality of any regulation of it must be measured by reference to the First Amendment. In some circumstances, however, the phrase connotes also that the standard for measurement is the most exacting level available….

[55] Defendants first attack Section 1201(a)(2), the anti-trafficking provision, as applied to them on the theory that DeCSS is constitutionally protected expression and that the statute improperly prevents them from communicating it. Their attack presupposes that a characterization of code as constitutionally protected subjects any regulation of code to the highest level of First Amendment scrutiny. As we have seen, however, this does not necessarily follow….

[56] Broadly speaking, restrictions on expression fall into two categories. Some are restrictions on the voicing of particular ideas, which typically are referred to as content based restrictions. Others have nothing to do with the content of the expression—i.e., they are content neutral—but they have the incidental effect of limiting expression.

[57] In general, government has no power to restrict expression because of its message, its ideas, its subject matter, or its content…. In consequence, content based restrictions on speech are permissible only if they serve compelling state interests by the least restrictive means available.

[58] Content neutral restrictions, in contrast, are measured against a less exacting standard. Because restrictions of this type are not motivated by a desire to limit the message, they will be upheld if they serve a substantial governmental interest and restrict First Amendment freedoms no more than necessary….

[59] The reason that Congress enacted the anti-trafficking provision of the DMCA had nothing to do with suppressing particular ideas of computer programmers and everything to do with functionality—with preventing people from circumventing technological access control measures—just as laws prohibiting the possession of burglar tools have nothing to do with preventing people from expressing themselves by accumulating what to them may be attractive assortments of implements and everything to do with preventing burglaries. Rather, it is focused squarely upon the effect of the distribution of the functional capability that the code provides. Any impact on the dissemination of programmers' ideas is purely incidental to the overriding concerns of promoting the distribution of copyrighted works in digital form while at the same time protecting those works from piracy and other violations of the exclusive rights of copyright holders….

[60] Congress is not powerless to adopt content neutral regulations that incidentally affect expression, including the dissemination of the functional capabilities of computer code. A sufficiently important governmental interest in seeing to it that computers are not instructed to perform particular functions may justify incidental restrictions on the dissemination of the expressive elements of a program. Such a regulation will be upheld if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.

[61] Moreover, to satisfy this standard, a regulation need not be the least speech-restrictive means of advancing the Government's interests. Rather, the requirement of narrow tailoring is satisfied so long as the regulation promotes a substantial government interest that would be achieved less effectively absent the regulation.

[62] The anti-trafficking provision of the DMCA furthers an important governmental interest—the protection of copyrighted works stored on digital media from the vastly expanded risk of piracy in this electronic age. The substantiality of that interest is evident both from the fact that the Constitution specifically empowers Congress to provide for copyright protection and from the significance to our economy of trade in copyrighted materials. Indeed, the Supreme Court has made clear that copyright protection itself is the engine of free expression. That substantial interest, moreover, is unrelated to the suppression of particular views expressed in means of gaining access to protected copyrighted works. Nor is the incidental restraint on protected expression—the prohibition of trafficking in means that would circumvent controls limiting access to unprotected materials or to copyrighted materials for noninfringing purposes—broader than is necessary to accomplish Congress' goals of preventing infringement and promoting the availability of content in digital form….

[63] Defendants' second focus is the contention that Section 1201(a)(2) is unconstitutional because it prevents others from making fair use of copyrighted works by depriving them of the means of circumventing plaintiffs' access control system. In substance, they contend that the anti-trafficking provision leaves those who lack sufficient technical expertise to circumvent CSS themselves without the means of acquiring circumvention technology that they need to make fair use of the content of plaintiffs' copyrighted DVDs….

[64] The DMCA does have a notable potential impact on uses that copy portions of a DVD movie because compliant DVD players are designed so as to prevent copying. In consequence, even though the fair use doctrine permits limited copying of copyrighted works in appropriate circumstances, the CSS encryption of DVD movies, coupled with the characteristics of licensed DVD players, limits such uses absent circumvention of CSS. Moreover, the anti-trafficking provision of the DMCA may prevent technologically unsophisticated persons who wish to copy portions of DVD movies for fair use from obtaining the means of doing so. It is the

interests of these individuals upon which defendants rely most heavily in contending that the DMCA violates the First Amendment because it deprives such persons of an asserted constitutional right to make fair use of copyrighted materials.

[65] As the foregoing suggests, the interests of persons wishing to circumvent CSS in order to make lawful use of the copyrighted movies it protects are remarkably varied. Some presumably are technologically sophisticated and therefore capable of circumventing CSS without access to defendants' or other purveyors' decryption programs; many presumably are not. Many of the possible fair uses may be made without circumventing CSS while others, i.e., those requiring copying, may not. Hence, the question whether Section 1201(a)(2) as applied here substantially affects rights, much less constitutionally protected rights, of members of the "fair use community" cannot be decided *in bloc,* without consideration of the circumstances of each member or similarly situated groups of members. Thus, the prudential concern with ensuring that constitutional questions be decided only when the facts before the Court so require counsels against permitting defendants to mount an overbreadth challenge here….

NOTES

1. Do you agree with the court's characterization of CSS as an "access control"? Can (or should) the § 1201 category into which CSS falls be assessed separately from the holistic strategy of which CSS is a part? An aspect of that strategy was to license use of CSS only to manufacturers who agreed not to equip their DVD players with a digital output. So is CSS better characterized as part of a "rights control" strategy? If CSS were characterized as a "rights control" technology, what effect, if any, on the court's decision? For an argument that courts have treated such hybrid or "merged" anti-circumvention technologies as entitled to the legal protections afforded to *both* access and rights controls, see R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERK. TECH. L.J. 619 (2003).

2. CSS also functions to enforce territorial restrictions on the playback of DVDs. That is, DVD players contain codes that restrict playback to DVDs marketed in certain territories. The purpose of the territorial restrictions is to enforce geographic price discrimination. For example, the copyright owner may charge a higher price for a motion picture on DVD in a relatively rich territory (such as North America), versus one that is less well-off (such as India). Is this a desirable use of technological protections? Does it advance the policy goals of the Copyright Act? Why or why not? For an argument that the DVD territorial restrictions are likely to restrict competition and harm social welfare, see Emily Dunt, Joshua S. Gans & Stephen P. King, *The Economic Consequences of DVD Regional Restrictions*, 21 ECON. PAPERS 32 (2002).

3. Review § 1201(a)(3), and also review § 1201(i). Now consider, in light of those provisions, the following questions. If a friend gives you his password to access the *New York Times* website, and you use that password to access the site without yourself purchasing an online subscription, are you circumventing a technological measure? What about if you read nine of the ten free monthly articles that the *New York Times* website permits you to access, and then clear your browser cache so that you can read more articles without purchasing a subscription? Have you circumvented a technological measure within the meaning of the statute? What about if you use Google Chrome's "Incognito Mode" to access articles on the *New York Times* website? Does your use of this feature, which prevents the *New York Times* from keeping count of the articles you view, constitute a circumvention of a technological measure?

4. Do you accept the *Reimerdes* court's argument that the anti-circumvention provisions are not limited by fair use? Review § 1201(c). Why do you think Congress included the language providing that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title"? On appeal, the Second Circuit gave this account of the function of § 1201(c): "[S]ubsection 1201(c)(1) … 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." Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443 (2d Cir. 2001). Do you agree with that interpretation?

5. The Second Circuit's decision on appeal in *Reimerdes*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001), also explored the limits of fair use as a "right of access":

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

6. Note a potentially important imprecision in the text of § 1201. Specifically, § 1201(a)(1)(A) provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." What does it mean for a technological measure to control access to "a work protected under this title"? The question becomes pressing when we consider whether an individual can circumvent access protections to copy a *public domain* work. Such a work is not "protected under this title," that is, under Title 17, in which the Copyright Act is codified. On one reading of the statutory text, individuals would be entitled to circumvent technological protections that control access to a public domain work. But perhaps there is another reading of the statute that focuses not on the work, but on the particular technological protection measure. If the measure controls access to "a"—that is, to *any*—work protected by copyright, then by this reading it is unlawful for an individual to circumvent it. Which reading of the statute do you think is correct? And why?

---

3. Second-Generation DMCA Disputes

Unlike *Reimerdes*, which arose out of efforts to protect against the piracy of copyrighted works, a second wave of DMCA disputes, exemplified by the next two cases, featured use of the DMCA in a bid to limit competition in certain product markets—specifically, in aftermarkets for complementary products (replacement garage door opener remote controls in the first case and replacement inkjet printer cartridges in the second one).

As you read these cases, ask yourself whether the use made of the DMCA is consistent with the policies underlying the Copyright Act. Is Congress likely to have either foreseen or approved such uses of the DMCA when it added the anti-circumvention provisions to the copyright law? Ask yourself also whether the ways in which the following opinions limit the scope of the DMCA are themselves subject to (metaphorical) circumvention by shifting legal and business strategies.

Chamberlain Group, Inc. v. Skylink Technologies, Inc.

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

GAJARSA, J.:

[1] The Chamberlain Group, Inc. appeals the … summary judgment of the United States District Court for the Northern District of Illinois in favor of Skylink Technologies, Inc., finding that Skylink is not violating the anti-trafficking provisions of the Digital Millennium Copyright Act, and dismissing all other claims, including claims of patent infringement….

[2] Chamberlain's claims at issue stem from its allegation that the District Court incorrectly construed the DMCA as placing a burden upon Chamberlain to prove that the circumvention of its technological measures enabled unauthorized access to its copyrighted software. But Skylink's accused device enables only uses that copyright law explicitly authorizes, and is therefore presumptively legal. Chamberlain has neither proved nor alleged a connection between Skylink's accused circumvention device and the protections that the copyright laws afford Chamberlain capable of overcoming that presumption. Chamberlain's failure to meet this burden alone compels a legal ruling in Skylink's favor. We therefore affirm the District Court's summary judgment in favor of Skylink….

[3] …. 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 District Court first denied Chamberlain's motion for summary judgment of its DMCA claim, and then granted Skylink's motion for summary judgment on the DMCA claim….

[4] 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.

[5] 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. Chamberlain places no explicit restrictions on the types of transmitter that the homeowner may use with its system at the time of purchase. Chamberlain's customers therefore assume that they enjoy all of the rights associated with the use of their GDOs and any software embedded therein that the copyright laws and other laws of commerce provide.

[6] 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 anticircumvention provisions, specifically § 1201(a)(2).

[7] The code in a standard (i.e., non-rolling code) GDO transmitter is unique but fixed. Thus, according to Chamberlain, the typical GDO is vulnerable to attack by burglars who can open the garage door using a "code grabber." According to Chamberlain, code grabbers allow burglars in close proximity to a homeowner operating her garage door to record the signal sent from the transmitter to the opener, and to return later, replay the recorded signal, and open the garage door. Chamberlain concedes, however, that code grabbers are more theoretical than practical burgling devices; none of its witnesses had either firsthand knowledge of a single code grabbing problem or familiarity with data demonstrating the existence of a problem. Nevertheless, Chamberlain claims to have developed its rolling code system specifically to prevent code grabbing.

[8] The essence of the rolling code system is that the transmitted signals are broken into fixed and variable (or "rolling") components. The entire transmitted signal is a bit string. The fixed component serves to identify the transmitter. The rolling component cycles through a lengthy cycle of bit strings only some of which are capable of opening the door at any given time, ostensibly so that a burglar replaying a grabbed code is unlikely to send a valid signal—and therefore unlikely to open the garage door.

[9] A user wishing to set up a new transmitter for use with her Security+ GDO must switch the opener to "program mode" and send a signal from the transmitter to the opener. The opener stores both the fixed and rolling components of the transmitted signal. When the user switches the opener back to "operate mode," the system is set and the user may operate the opener with the newly programmed transmitter. In Chamberlain's transmitter, a computer program increases the rolling code by a factor of three each time the user activates the transmitter. When the transmitted signal reaches the receiver, a program in the opener checks to see whether the rolling code received was identical to one of the most recently received 1,024 rolling codes (the "rear window"). If so, it will not activate the motor. If, on the other hand, the rolling code received is among the next 4,096 binary signals (the "forward window"), the receiver will activate the motor.

[10] Not all recognized binary rolling signals are in either the forward or rear windows. If the transmitter sends a *single* signal outside of either window, the receiver will ignore it. If, however, the transmitter sends *two* signals outside either window in rapid succession, the opener will again access its programming, this time to determine whether the two signals together comprise a "resynchronization" sequence. If the signals differ by three, the receiver will reset the windows and activate the motor. According to Chamberlain, resynchronization accommodates the possibility that homeowners using the same transmitter for multiple residences may transmit so many signals while out of range of the opener that they exhaust the entire forward window.

[11] Skylink began marketing and selling universal transmitters in 1992. Skylink designed its Model 39, launched in August 2002, to interoperate with common GDOs, including both rolling code and non-rolling code GDOs. Although Chamberlain concedes that the Model 39 transmitter is capable of operating many different GDOs, it nevertheless asserts that Skylink markets the Model 39 transmitter for use in circumventing its copyrighted rolling code computer program. Chamberlain supports this allegation by pointing to the Model 39's setting that operates *only* Chamberlain's rolling code GDOs.

[12] Skylink's Model 39 *does not* use rolling code technology.... When the homeowner actually uses the transmitter, it broadcasts *three* fixed codes in rapid succession. The first binary signal combines the identifying component with an arbitrary binary sequence. The second binary signal subtracts 1800 from the first signal. The third signal adds three to the second signal. The combination of these three codes transmitted with every press of the Model 39 transmitter button will either cause the Chamberlain GDO to operate in response to the first fixed code or cause the GDO to resynchronize and operate in response to the second and third fixed codes. Chamberlain characterizes this procedure as a circumvention of an important security measure; a code grabber that recorded the Model 39's three codes could later play them back and activate a Chamberlain rolling code GDO without authorization.

[13] .... [I]t is ... noteworthy that Chamberlain *has not* alleged either that Skylink infringed its copyright or that Skylink is liable for contributory copyright infringement. What Chamberlain *has* alleged is that because its opener and transmitter both incorporate computer programs "protected by copyright" and because rolling codes are a "technological measure" that "controls access" to those programs, Skylink is prima facie liable for violating § 1201(a)(2). In the District Court's words, "Chamberlain claims that the rolling code computer program has a protective measure that protects itself. Thus, only one computer program is at work here, but it has two functions: (1) to verify the rolling code; and (2) once the rolling code is verified, to activate the GDO motor, by sending instructions to a microprocessor in the GDO." ...

[14] The essence of the DMCA's anticircumvention provisions is that §§ 1201(a), (b) establish causes of action for liability. They do not establish a new property right. The DMCA's text indicates that circumvention is not infringement, 17 U.S.C. § 1201(c)(1) ("Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."), and the statute's structure makes the point even clearer. This distinction between property and liability is critical. Whereas copyrights, like patents, are property, liability protection from unauthorized circumvention merely creates a new cause of action under which a defendant may be liable. The distinction between property and liability goes straight to the issue of authorization, the issue upon which the District Court both denied Chamberlain's and granted Skylink's motion for summary judgment.

[15] A plaintiff alleging copyright infringement need prove *only* (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original. The existence of a license, exclusive or nonexclusive, creates an affirmative defense to a claim of copyright infringement. In other words, under Seventh Circuit copyright law, a plaintiff only needs to show that the defendant has used her property; the burden of proving that the use was authorized falls squarely on the defendant. The DMCA, however, *defines* circumvention as an activity undertaken "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). The plain language of the statute therefore requires a plaintiff alleging circumvention (or trafficking) to prove that the defendant's access was unauthorized—a significant burden where, as here, the copyright laws authorize consumers to use the copy of Chamberlain's software embedded in the GDOs that they purchased....

[16] .... According to Chamberlain, the 1998 enactment of the DMCA .... overrode all pre-existing consumer expectations about the legitimate uses of products containing copyrighted embedded software. Chamberlain contends that Congress empowered manufacturers to prohibit consumers from using embedded software products in conjunction with competing products when it passed § 1201(a)(1). According to Chamberlain, *all* such uses of products containing copyrighted software to which a technological measure controlled access are now per se illegal under the DMCA unless the manufacturer provided consumers with *explicit* authorization....

[17] Such an exemption, however, is only plausible if the anticircumvention provisions established a new property right ...—which as we have already explained, they do not.... Contrary to Chamberlain's assertion, the DMCA emphatically *did not* "fundamentally alter" the legal landscape governing the reasonable expectations

of consumers or competitors; *did not* "fundamentally alter" the ways that courts analyze industry practices; and *did not* render the pre-DMCA history of the GDO industry irrelevant.

[18] What the DMCA did was introduce new grounds for liability in the context of the unauthorized access of copyrighted material. The statute's plain language requires plaintiffs to prove that those circumventing their technological measures controlling access did so "without the authority of the copyright owner." 17 U.S.C. § 1201(3)(A). Our inquiry ends with that clear language. We note, however, that the statute's structure, legislative history, and context within the Copyright Act all support our construction. They also help to explain why Chamberlain's warranty conditions and website postings cannot render users of Skylink's Model 39 "unauthorized" users for the purposes of establishing trafficking liability under the DMCA....

[19] 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." ...

[20] 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.

[21] Chamberlain derives its strongest claimed support for its proposed construction from the trial court's opinion in *Reimerdes,* 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....

[22] 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. Chamberlain's repeated reliance on language targeted at defendants trumpeting their "electronic civil disobedience" apparently led it to misconstrue significant portions of the DMCA. Many of Chamberlain's assertions in its brief to this court conflate the property right of copyright with the liability that the anticircumvention provisions impose.

[23] Chamberlain relies upon the DMCA's prohibition of "fair uses ... as well as foul" 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 attempts to deal with special problems created by the so-called digital revolution....

[24] .... 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. 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.

[25] 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, 537 U.S. 186, 205 n.10 (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." *Id.* at 204–05 (emphasis added). 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.

[26] 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 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....

[27] Chamberlain's proposed severance of "access" from "protection" in § 1201(a) creates numerous other problems.... 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.

[28] 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....

[29] Finally, the requisite "authorization," on which the District Court granted Skylink summary judgment, points to yet another inconsistency in Chamberlain's proposed construction. The notion of authorization is central to understanding § 1201(a). 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….

[30] 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. *See* H.R. REP. NO. 105–551, at 26 (1998). The courts must adhere to the language that Congress enacted to determine how it attempted to achieve that balance….

[31] 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….

[32] Chamberlain … has failed to show not only the requisite lack of authorization, but also the necessary fifth element of its claim, the critical nexus between access and protection. Chamberlain neither alleged copyright infringement *nor explained how the access provided by the Model 39 transmitter facilitates the infringement of any right that the Copyright Act protects.* There can therefore be no reasonable relationship between the access that homeowners gain to Chamberlain's copyrighted software when using Skylink's Model 39 transmitter and the protections that the Copyright Act grants to Chamberlain. The Copyright Act authorized Chamberlain's customers to use the copy of Chamberlain's copyrighted software embedded in the GDOs that they purchased. Chamberlain's customers are therefore immune from § 1201(a)(1) circumvention liability. In the absence of allegations of either copyright infringement or § 1201(a)(1) circumvention, Skylink cannot be liable for § 1201(a)(2) trafficking. The District Court's grant of summary judgment in Skylink's favor was correct. Chamberlain failed to allege a claim under 17 U.S.C. § 1201….

[33] The DMCA does not create a new property right for copyright owners. Nor, for that matter, does it divest the public of the property rights that the Copyright Act has long granted to the public. The anticircumvention and anti-trafficking provisions of the DMCA create new grounds of liability. A copyright owner seeking to impose liability on an accused circumventor must demonstrate a reasonable relationship between the circumvention at issue and a use relating to a property right for which the Copyright Act permits the copyright owner to withhold authorization—as well as notice that authorization was withheld. A copyright owner seeking to impose liability on an accused trafficker must demonstrate that the trafficker's device enables either copyright infringement or a prohibited circumvention. Here, the District Court correctly ruled that Chamberlain pled no connection between unauthorized use of its copyrighted software and Skylink's accused transmitter. This connection is critical to sustaining a cause of action under the DMCA. We therefore affirm the District Court's summary judgment in favor of Skylink….

Lexmark International, Inc. v. Static Control Components, Inc.

387 F.3d 522 (6th Cir. 2005)

SUTTON, J.:

[1] This copyright dispute involves two computer programs, two federal statutes and three theories of liability. The first computer program, known as the "Toner Loading Program," calculates toner level in printers manufactured by Lexmark International. The second computer program, known as the "Printer Engine Program," controls various printer functions on Lexmark printers.

[2] The first statute, the general copyright statute, 17 U.S.C. § 101 *et seq.,* ... grants copyright protection to "original works of authorship fixed in any tangible medium of expression," but does not "extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery." The second federal statute, the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.,* was enacted in 1998 and proscribes the sale of products that may be used to "circumvent a technological measure that effectively controls access to a work" protected by the copyright statute.

[3] These statutes became relevant to these computer programs when Lexmark began selling discount toner cartridges for its printers that only Lexmark could re-fill and that contained a microchip designed to prevent Lexmark printers from functioning with toner cartridges that Lexmark had not re-filled. In an effort to support the market for competing toner cartridges, Static Control Components (SCC) mimicked Lexmark's computer chip and sold it to companies interested in selling remanufactured toner cartridges.

[4] Lexmark brought this action to enjoin the sale of SCC's computer chips and raised three theories of liability in doing so. Lexmark claimed that SCC's chip copied the Toner Loading Program in violation of the federal copyright statute. It claimed that SCC's chip violated the DMCA by circumventing a technological measure designed to control access to the Toner Loading Program. And it claimed that SCC's chip violated the DMCA by circumventing a technological measure designed to control access to the Printer Engine Program.

[5] After an evidentiary hearing, the district court decided that Lexmark had shown a likelihood of success on each claim and entered a preliminary injunction against SCC. As we view Lexmark's prospects for success on each of these claims differently, we vacate the preliminary injunction and remand the case for further proceedings....

[6] **The Parties.** Headquartered in Lexington, Kentucky, Lexmark is a leading manufacturer of laser and inkjet printers and has sold printers and toner cartridges for its printers since 1991. Lexmark is a publicly traded corporation and reported $4.8 billion in revenue for 2003.

[7] Static Control Components is a privately held company headquartered in Sanford, North Carolina. Started in 1987, it currently employs approximately 1,000 workers and makes a wide range of technology products, including microchips that it sells to third-party companies for use in remanufactured toner cartridges.

[8] **The Two Computer Programs.** The first program at issue is Lexmark's "Toner Loading Program," which measures the amount of toner remaining in the cartridge based on the amount of torque (rotational force) sensed on the toner cartridge wheel.... The Toner Loading Program for [one set of] printers comprises 33 program instructions and occupies 37 bytes of memory, while the Toner Loading Program for [another set of] printers comprises 45 program commands and uses 55 bytes of memory. To illustrate the modest size of this computer program, the phrase "Lexmark International, Inc. vs. Static Control Components, Inc." in ASCII format would occupy more memory than either version of the Toner Loading Program. The Toner Loading Program is located on a microchip contained in Lexmark's toner cartridges.

[9] The second program is Lexmark's "Printer Engine Program." The Printer Engine Program occupies far more memory than the Toner Loading Program and translates into over 20 printed pages of program commands. The program controls a variety of functions on each printer—e.g., paper feed and movement, and printer motor control. Unlike the Toner Loading Program, the Printer Engine Program is located within Lexmark's printers.

[10] Lexmark obtained Certificates of Registration from the Copyright Office for both programs. Neither program is encrypted and each can be read (and copied) directly from its respective memory chip.

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

[12] To ensure that consumers adhere to the Prebate agreement, Lexmark uses an "authentication sequence" that performs a "secret handshake" between each Lexmark printer and a microchip on each Lexmark toner cartridge. Both the printer and the chip employ a publicly available encryption algorithm known as "Secure Hash Algorigthm–1" or "SHA–1," which calculates a "Message Authentication Code" based on data in the microchip's memory. If the code calculated by the microchip matches the code calculated by the printer, the printer functions normally. If the two values do not match, the printer returns an error message and will not operate, blocking consumers from using toner cartridges that Lexmark has not authorized.

[13] **SCC's Competing Microchip.** SCC sells its own microchip—the "SMARTEK" chip—that permits consumers to satisfy Lexmark's authentication sequence each time it would otherwise be performed, *i.e.*, when the printer is turned on or the printer door is opened and shut. SCC's advertising boasts that its chip breaks Lexmark's "secret code" (the authentication sequence), which "even on the fastest computer available today … would take **Years** to run through all of the possible 8–byte combinations to break." SCC sells these chips to third-party cartridge remanufacturers, permitting them to replace Lexmark's chip with the SMARTEK chip on refurbished Prebate cartridges. These recycled cartridges are in turn sold to consumers as a low-cost alternative to new Lexmark toner cartridges.

[14] Each of SCC's SMARTEK chips also contains a copy of Lexmark's Toner Loading Program, which SCC claims is necessary to make its product compatible with Lexmark's printers. The SMARTEK chips thus contain an identical copy of the Toner Loading Program that is appropriate for each Lexmark printer, and SCC acknowledges that it "slavishly copied" the Toner Loading Program "in the exact format and order" found on Lexmark's cartridge chip….

{In a part of the opinion, omitted here, the court found that the district court had erred in finding that Lexmark's Toner Loading Program was copyrightable. The court found that the program was functional, that elements of the program were likely scenes a faire or merged with functional aspects, that any creativity that remained was likely de minimis, and that in any event SCC's use was likely fair use.}

[15] In filing its complaint and in its motion for a preliminary injunction, Lexmark invoked … the ban on distributing devices that circumvent access-control measures placed on copyrighted works. *See* 17 U.S.C. § 1201(a)(2). According to Lexmark, SCC's SMARTEK chip is a "device" marketed and sold by SCC that "circumvents" Lexmark's "technological measure" … which "effectively controls access" to its copyrighted works (the Toner Loading Program and Printer Engine Program). Lexmark claims that the SMARTEK chip meets all three tests for liability under § 1201(a)(2): (1) the chip "is primarily designed or produced for the

purpose of circumventing" Lexmark's authentication sequence, 17 U.S.C. § 1201(a)(2)(A); (2) the chip "has only limited commercially significant purpose or use other than to circumvent" the authentication sequence, *id.* § 1201(a)(2)(B); and (3) SCC "market[s]" the chip "for use in circumventing" the authentication sequence, *id.* § 1201(a)(2)(C). The district court agreed and concluded that Lexmark had shown a likelihood of success under all three provisions….

[16] We initially consider Lexmark's DMCA claim concerning the Printer Engine Program, which (the parties agree) is protected by the general copyright statute. In deciding that Lexmark's authentication sequence "effectively controls access to a work protected under [the copyright provisions]," the district court relied on a definition in the DMCA saying that a measure "effectively controls access to a work" if, "in the ordinary course of operation," it "requires the application of information, or a process or treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3). Because Congress did not explain what it means to "gain access to the work," the district court relied on the "ordinary, customary meaning" of "access": "the ability to enter, to obtain, or to make use of." Based on this definition, the court concluded that "Lexmark's authentication sequence effectively 'controls access' to the Printer Engine Program because it controls the consumer's ability to *make use of* these programs."

[17] We disagree. It is not Lexmark's authentication sequence that "controls access" to the Printer Engine Program. It is the purchase of a Lexmark printer that allows "access" to the program. Anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence, and the data from the program may be translated into readable source code after which copies may be freely distributed. No security device, in other words, protects access to the Printer Engine Program Code and no security device accordingly must be circumvented to obtain access to that program code.

[18] The authentication sequence, it is true, may well block one form of "access"—the "ability to … make use of" the Printer Engine Program by preventing the printer from functioning. But it does not block another relevant form of "access"—the "ability to [] obtain" a copy of the work or to "make use of" the literal elements of the program (its code). Because the statute refers to "control[ling] access to a work protected under this title," it does not naturally apply when the "work protected under this title" is otherwise accessible. 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 also 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….

[19] … Lexmark counters that several cases have embraced a "to make use of" definition of "access" in applying the DMCA. While Lexmark is partially correct, these cases (and others as well) ultimately illustrate the liability line that the statute draws and in the end explain why access to the Printer Engine Program is not covered.

[20] In the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code's execution. For example, the encoded data on CDs translates into music and on DVDs into motion pictures, while the program commands in software for video games or computers translate into some other visual and audio manifestation. In the cases upon which Lexmark relies, restricting "use" of the work means restricting consumers from making use of the copyrightable expression in the work….

[21] The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or DVDs, "using" or executing the Printer Engine Program does not in turn create any protected expression. Instead, the program's output is purely functional: the Printer Engine Program controls a number of operations in the Lexmark printer such as paper feed, paper movement, and motor control. And unlike the code underlying video games or DVDs, no encryption or other technological measure prevents access to the Printer Engine Program. Presumably, it is precisely because the Printer Engine Program is not a conduit to protectable expression that explains why Lexmark (or any other printer company) would not block access to the computer software that makes the printer work. Because Lexmark's authentication sequence does not restrict access to this literal code, the DMCA does not apply.

[22] Lexmark next argues that access-control measures may "effectively control access" to a copyrighted work within the meaning of the DMCA even though the measure may be evaded by an enterprising end-user. Doubtless, Lexmark is correct that a precondition for DMCA liability is not the creation of an impervious shield to the copyrighted work. Otherwise, the DMCA would apply only when it is not needed.

[23] But our reasoning does not turn on the *degree* to which a measure controls access to a work. It turns on the textual requirement that the challenged circumvention device must indeed circumvent *something,* which did not happen with the Printer Engine Program. Because Lexmark has not directed any of its security efforts, through its authentication sequence or otherwise, to ensuring that its copyrighted work (the Printer Engine Program) cannot be read and copied, it cannot lay claim to having put in place a "technological measure that effectively controls access to a work protected under [the copyright statute]." 17 U.S.C. § 1201(a)(2)(B).

[24] Nor can Lexmark tenably claim that this reading of the statute fails to respect Congress's purpose in enacting it. Congress enacted the DMCA to implement the Copyright Treaty of the World Intellectual Property Organization, and in doing so expressed concerns about the threat of "massive piracy" of digital works due to "the ease with which [they] can be copied and distributed worldwide virtually instantaneously." S. REP. NO. 105–190, at 8 (1998). As Congress saw it, "copyrighted works will most likely be encrypted and made available to consumers once payment is made for access to a copy of the work. [People] will try to profit from the works of others by decoding the encrypted codes protecting copyrighted works, or engaging in the business of providing devices or services to enable others to do so." H.R. REP. NO. 105–551, pt. 1, at 10. Backing with legal sanctions "the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections," Congress noted, would encourage copyright owners to make digital works more readily available, *see* S. REP. NO. 105–190, at 8.

[25] Nowhere in its deliberations over the DMCA did Congress express an interest in creating liability for the circumvention of technological measures designed to prevent consumers from using consumer goods while leaving the copyrightable content of a work unprotected….

[26] In view of our conclusion regarding the Printer Engine Program, we can dispose quickly of Lexmark's DMCA claim regarding the Toner Loading Program. The SCC chip does not provide "access" to the Toner Loading Program but replaces the program. And to the extent a copy of the Toner Loading Program appears on the Printer Engine Program, Lexmark fails to overcome the same problem that undermines its DMCA claim with respect to the Printer Engine Program: Namely, it is not the SCC chip that permits access to the Printer Engine Program but the consumer's purchase of the printer. One other point deserves mention. All three liability provisions of this section of the DMCA require the claimant to show that the "technological measure" at issue "controls access to *a work protected under this title,*" *see* 17 U.S.C. § 1201(a)(2)(A)-(C), which is to say a work protected under the general copyright statute. To the extent the Toner Loading Program is not a "work protected under [the copyright statute]," … the DMCA necessarily would not protect it….

[27] Because Lexmark failed to establish a likelihood of success on any of its claims, whether under the general copyright statute or under the DMCA, we vacate the district court's preliminary injunction and remand the case for further proceedings consistent with this opinion.

MERRITT, J., concurring. ...

[28] I write separately to emphasize that our holding should not be limited to the narrow facts surrounding either the Toner Loading Program or the Printer Engine Program. We should make clear that in the future companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods for themselves just by tweaking the facts of this case: by, for example, creating a Toner Loading Program that is more complex and "creative" than the one here, or by cutting off other access to the Printer Engine Program. The crucial point is that the DMCA forbids anyone from trafficking in any technology that "is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [protected] work." 17 U.S.C. § 1201(2)(A) (emphasis added). The key question is the "purpose" of the circumvention technology. The microchip in SCC's toner cartridges is intended not to reap any benefit from the Toner Loading Program—SCC's microchip is not designed to measure toner levels—but only for the purpose of making SCC's competing toner cartridges work with printers manufactured by Lexmark.

[29] By contrast, Lexmark would have us read this statute in such a way that any time a manufacturer intentionally circumvents any technological measure and accesses a protected work it necessarily violates the statute regardless of its "purpose." Such a reading would ignore the precise language—"for the purpose of"—as well as the main point of the DMCA—to prohibit the pirating of copyright-protected works such as movies, music, and computer programs. If we were to adopt Lexmark's reading of the statute, manufacturers could potentially create monopolies for replacement parts simply by using similar, but more creative, lock-out codes. Automobile manufacturers, for example, could control the entire market of replacement parts for their vehicles by including lock-out chips. Congress did not intend to allow the DMCA to be used offensively in this manner, but rather only sought to reach those who circumvented protective measures "for the purpose" of pirating works protected by the copyright statute. Unless a plaintiff can show that a defendant circumvented protective measures for such a purpose, its claim should not be allowed to go forward. If Lexmark wishes to utilize DMCA protections for (allegedly) copyrightable works, it should not use such works to prevent competing cartridges from working with its printer....

FEIKENS, J., Concurring in part and Dissenting in part. {omitted}

NOTES

1. *Chamberlain* reads § 1201 to bar access only when the access is related to infringement. In *MDY Industries, LLC v. Blizzard Entertainment*, *Inc.*, 629 F.3d 928 (9th Cir. 2011), the Ninth Circuit rejected that reading of the statute. *MDY* concluded that § 1201(a) extends "a new form of protection, i.e., the right to prevent circumvention of access controls" to copyrighted works without regard to whether access is connected to infringement. *Id.* at 945. Which court's interpretation is a better fit with the text of § 1201? Which court's approach is more consistent with the goals of copyright law?

2. *Chamberlain* also holds that the plaintiff has in effect "authorized" the defendant's customers to access and use their copyrighted software. Do you agree with this holding? Is there anything the plaintiff could do to evade its effect?

3. *Lexmark* holds that Lexmark's identification sequence does not control access to the Printer Engine Program, because that program is itself not encrypted and may be copied directly from the printer memory. Do you agree with this holding? Again, is there anything the plaintiff could do to evade its effect?

4. The plaintiffs in both *Chamberlain* and *Lexmark* were attempting to use the DMCA not principally to protect valuable copyrighted works but as a lever to limit competition. How do you think that fact affected the courts' interpretations of the meaning of § 1201? Do you see any reason to distinguish between the strategy employed by Chamberlain and the one employed by Lexmark?

5. Note that the DMCA also provides legal protection for so-called "copyright management information" (CMI), as discussed in Chapter V with regard to attribution. Recall that the statute defines "copyright management information" to include such information or "metadata" about a copyrighted work as the information in the copyright notice (©, year of creation, and identity of the copyright owner), the title, the identity of the author (if different from the copyright owner), and the terms of use. The DMCA's CMI protections, codified in § 1202, provide as follows:

> *(a) False Copyright Management Information.—No person shall knowingly and with the intent to induce, enable, facilitate, or conceal infringement—(1) provide copyright management information that is false, or (2) distribute or import for distribution copyright management information that is false.*
>
> *(b) Removal or Alteration of Copyright Management Information.—No person shall, without the authority of the copyright owner or the law—(1) intentionally remove or alter any copyright management information, (2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or (3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law—knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title.*

Some courts have read § 1202 to apply only to CMI located *on or in* a copyrighted work, and not such information that is merely *associated with* a copyrighted work. In *Kelly v. Arriba Soft Corp.*, 77 F. Supp. 2d 1116, 1121-22 (C.D. Cal. 1999), *rev'd and remanded in part on other grounds*, 336 F.3d 811 (9th Cir. 2003), the plaintiff photographer included CMI adjacent to his photographs, but not directly on them. The court granted summary judgment in favor of the defendant, whose copies of the photographs had removed the CMI. The court held that "[b]ased on the language and the structure of the statute, … this provision applies only to the removal of copyright management information on a plaintiff's product or original work." *Id.* at 1122. But other courts have disagreed. Notably, in *Murphy v. Millennium Radio Group L.L.C.*, 650 F.3d 295, 305, 310 (3d Cir. 2011), the Third Circuit concluded that the location of the photographer's name in the printed "gutter" credit did not prevent it from qualifying as CMI, and that the defendant's removal of the information could trigger liability under § 1202.

In *Stevens v. CoreLogic, Inc.*, 899 F.3d 666 (9th Cir. 2018), the Ninth Circuit affirmed a district court's grant of summary judgment for CoreLogic in an action brought under § 1202. Plaintiffs, professional real estate photographers, alleged that CoreLogic violated § 1202 by removing CMI from their photographs and distributing those photographs with the CMI removed. The Ninth Circuit held that liability under § 1202(b) requires an affirmative showing that the defendant knew the prohibited act would induce, enable, facilitate, or conceal infringement. The court held that the plaintiffs failed to make that showing because they produced no evidence that could show that CoreLogic knew its software carried even a substantial risk of inducing, enabling, facilitating, or concealing infringement, let alone a pattern or probability of such a connection to infringement.

In *Mango v. Buzzfeed, Inc.*, 970 F.3d 167 (2d Cir. 2020), the Second Circuit clarified the knowledge required to support civil liability under § 1202 for the removal or alteration of CMI. In that case, Buzzfeed distributed Gregory Mango's photograph knowing that the valid CMI had been removed and replaced with improper CMI. The court held that the statutory language does not require knowledge that removal of the CMI would facilitate third-party infringement. Rather, the statute requires (1) knowledge that CMI has been removed and altered,

and (2) knowledge that the removal or alteration will conceal "an infringement." The court found that Buzzfeed's distribution of Mango's photograph with knowledge that the CMI was removed and replaced with improper credit satisfied the first knowledge element. And Buzzfeed's knowing distribution of the photo with false attribution, which implied BuzzFeed had proper authorization to publish the photo and concealed its own infringement, satisfied the second knowledge element.

Finally, it appears that § 1202 claims have become more common in recent years. This may be because § 1203 of the Copyright Act makes statutory damages available for successful claims under § 1202 without regard to whether the relevant copyright was timely registered. *See* 17 U.S.C. § 1203(c)(3)(B) ("At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1202 in the sum of not less than $2,500 or more than $25,000.").
