Order Code RL32692

CRS Report for Congress
Received through the CRS Web

# Anticircumvention under the Digital Millennium Copyright Act and Reverse Engineering: Recent Legal Developments

**December 10, 2004**

Robin Jeweler
Legislative Attorney
American Law Division

# Anticircumvention under the Digital Millennium Copyright Act and Reverse Engineering: Recent Legal Developments

## Summary

The Digital Millennium Copyright Act (DMCA) prohibits individuals from manufacturing, selling, or trafficking in technology, products, services, or devices that circumvent technology designed to control access to a copyrighted work. This is known as the DMCA's "anticircumvention" provision. Although most commonly invoked in the context of digital piracy of music, motion pictures, and other entertainment-related media, another genre of anticircumvention-based cases is making its way through the courts. These cases involve the initiation of anticircumvention litigation for what some argue are anti-competitive purposes in the marketing and sale of durable goods.

The practice of reverse engineering allows others to identify and analyze the creative versus the functional aspects of copyrighted software and to utilize them to some degree. In some contexts, reverse engineering has been held by the courts to be a fair use of copyright-protected property. There is also an express, limited statutory exemption for reverse engineering under the DMCA. How the practice and use of reverse engineering for commercial goals relates to the relatively new protections against circumvention is of interest to many. They are concerned with the extent to which access-control technology is likely be employed to extend (or attempt to extend) a copyright holder's control over durable goods with copyrighted components and the secondary markets for such goods.

This report examines two recent decisions from U.S. Courts of Appeals, *Lexmark International, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004), and *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004). Both cases allege violation of the anticircumvention statute with respect to development and sale of consumer goods. In *Lexmark*, the defendant marketed a microchip that allowed third-party manufacturers to sell toner cartridges that worked with the plaintiff's printer. In *Chamberlain*, the defendant sold a universal garage door opener transmitter that worked with the plaintiff's garage door opener. In both cases, the courts found that the actions of the defendants did *not* violate the anticircumvention provisions of the DMCA. In doing so, the courts had to reconcile closely related aspects of copyright law with the strictures of the DMCA.

This report will not be updated.

## Contents

Background . . . . . 1
Exceptions to the copyright monopoly: reverse engineering . . . . . 2
Lexmark International v. Static Control Components, Inc . . . . . 4
Chamberlain Group, Inc. v. Skylink Technologies, Inc . . . . . 9
Conclusion . . . . . 15

# Anticircumvention under the Digital Millennium Copyright Act and Reverse Engineering: Recent Legal Developments

**Background.** The Digital Millennium Copyright Act (DMCA) prohibits individuals from manufacturing, selling, or trafficking in technology, products, services, or devices that circumvent technology designed to control access to a copyrighted work.[1] This is known as the DMCA's "anticircumvention" provision. Enacted in 1998, the law became effective in 2000. The DMCA's anticircumvention provisions have proven to be controversial. Proponents argue that they are essential to protect the creation and distribution of, and the market for digital intellectual property (IP), while critics argue that they extend the copyright monopoly beyond its intended scope and thwart the public's ability to access materials for permissible purposes.[2]

The statute is best known in the context of encryption programs and access control "gates" interposed between the public and copyrighted digital entertainment media, e.g., music and motion pictures.[3] Here, critics of the DMCA argue that the anticircumvention provisions allow copyright holders to impose new and overly restrictive conditions on content users. This new layer of IP protection has been referred to as "paracopyright."[4] It refers to the ability of content owners to use conditions for access in order to extend control over usage of copyrighted work.

The focus of this report, however, is another genre of anticircumvention-based cases making their way through the courts. These cases involve the initiation of anticircumvention litigation for what some argue are anti-competitive purposes in the marketing and sale of durable goods. The question is, when a manufacturer utilizes

---

[1] 17 U.S.C. § 1201 entitled "Circumvention of copyright protection systems."

[2] While a copyright owner's exclusive rights in a copyrighted work is set forth at 17 U.S.C. 106, exceptions to exclusive rights are set forth at, *e.g.,* 17 U.S.C. §§ 107, 108, 110, 111, 117.

[3] The statute was widely publicized in a successful suit by movie studios to prevent the posting over the Internet of a code to circumvent the Content Scrambling System, an encryption program for digital motion pictures. Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001).

[4] H.R. Rept. 105-551, Part 2, 105th Cong., 2d Sess. 24-25 (1998) quoting a letter from copyright law professors arguing that enactment of anticircumvention legislation "would represent an unprecedented departure into the zone of what might be called paracopyright – an uncharted new domain of legislative provisions designed to strengthen copyright protection by regulating conduct which traditionally has fallen outside the regulatory sphere of intellectual property law."

software as a "gate" to enable, control, or restrict access to consumer goods containing copyrighted material, to what extent does it preclude competitors from circumventing the controls in the engineering of compatible – or competitive – consumer goods?

This report examines two cases involving 17 U.S.C. § 1201 that involve commercial interests unrelated to the entertainment industry, specifically, manufacturers of garage door openers and manufacturers of toner cartridges for photocopying machines. These cases involve issues that have been the basis for criticism of the DMCA in a slightly different commercial context, namely, whether the provisions permit IP owners to extend their copyright monopoly beyond its intended scope to control consumer goods.

**Exceptions to the copyright monopoly: reverse engineering.** There are several statutory and judicially created exceptions to a copyright holder's right to control IP. Among the best known is the public's right to make "fair use" of a protected work.[5] Among the judicially-sanctioned interpretations of the fair use defense to copyright infringement is the right to "reverse engineer" a copyrighted computer program to gain an understanding of its unprotected functional elements.[6] Like all fair use analyses, the context for a court's decision is intensely fact-specific. But a court considering the legitimacy of reverse engineering as a fair use will factor in the public interest in a competitive marketplace for consumer goods. When, for example, copyrighted computer code functions primarily as a "lock out" code designed to prevent access to functional as opposed to copyrighted elements of a durable good, then reverse engineering or other methods of overcoming it may be permissible.[7]

In *Sega Enterprises Ltd. v. Accolade, Inc.*, [8] a U.S. Court of Appeals held that Accolade, Inc.'s disassembly and reverse engineering of Sega's copyrighted computer program was a fair use. Accolade reverse engineered the program in order to manufacture video games on cartridges that were compatible with Sega's video console, Genesis. Because there was no other known method of access, the court found that Accolade's use of Sega's initialization code did not violate the U.S. Copyright Act. Accolade's copies of Sega's software enabled it to discover the functional requirements for compatibility with the Genesis console. Even though Accolade's ultimate purpose was the development of Genesis-compatible games for sale, its direct use of the copyrighted material and its purpose in reverse engineering Sega's code was to study the *functional* requirements for Genesis compatibility.

---

[5] 17 U.S.C. § 107.

[6] Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1993); *See also* Sony Computer Entertainment v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000); Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1539 (11th Cir. 1996); Atari Games Corp. v. Nintendo, 975 F.2d 832, 843 (Fed. Cir. 1992).

[7] *See* Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs,* 68 S. CAL. L. REV. 1091 (1994-1995).

[8] 977 F.2d 1510 (9th Cir. 1993).

Accolade wanted to modify its existing games so that they could be played on the Genesis console. In reaching its decision, the court noted that

> [W]e are free to consider the public benefit resulting from a particular use notwithstanding the fact that the alleged infringer may gain commercially. Public benefit need not be direct or tangible, but may arise because the challenged use serves a public interest. In the case before us, Accolade's identification of the functional requirements for Genesis compatibility has led to an increase in the number of independently designed video game programs offered for use with the Genesis console. It is precisely this growth in creative expression, based on the dissemination of other creative works and the unprotected ideas contained in those works, that the Copyright Act was intended to promote.[9]

Judicial determination of what activity constitutes a fair use of copyrighted property is a fluid and evolving doctrine. The anticircumvention provisions of the DMCA, however, establish offenses wholly distinct from copyright infringement. In other words, reverse engineering that may be (or have been) permissible under the Copyright Act may no longer be permissible under the DMCA. To the extent that the DMCA's anticircumvention provisions address the narrow issue of manipulating – or circumventing – technology (whether or not it is copyrightable in its own right) *to access* copyrighted technology, its impact on fair use, particularly the employment of reverse engineering, may have a significant impact in the marketplace.

And, there are still many other legal doctrines that impact the legality of reverse engineering in any given context. For example, the DMCA itself, at 17 U.S.C. § 1201(f), contains an express exemption for reverse engineering "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs[.]"[10] Conversely, the courts have honored contractual terms under state law, such as licensing agreements and terms of use agreements, that curtail a user's right to reverse engineer copyrighted material.[11] How do the rights, remedies, and exceptions in the DMCA relate to comparable ones in the Copyright Act?

In the realm of online entertainment, such as music, film, and electronic books, critics of the DMCA argue that it has the potential to curtail the public's right to make fair use of copyrighted material. In other commercial contexts, litigants argue that the act's anticircumvention provisions may thwart access to the permissible fair use of reverse engineering and thereby permit a copyright holder to leverage a limited monopoly to control areas outside of that monopoly in the broader world of fungible consumer goods, a practice traditionally held in check by the judicial doctrine of

---

[9] *Id.* at 1523. (Citations omitted.)

[10] 17 U.S.C. § 1201(f)(1).

[11] *See* Bowers v. Baystate Technologies, Inc., 320 F.3d 1317 (Fed. Cir.), *cert. denied*, 539 U.S. 928 (2003)(Copyright Act did not preempt or narrow scope of a shrink wrap license agreement that prohibited reverse engineering.) *See also,* Davidson & Assoc., Inc. v. Internet Gateway, 334 F.Supp.2d 1164 (E.D.Mo. 2004).

"copyright misuse."[12] But with the "rebalancing" of interests that was effected by enactment of the DMCA, how far can a manufacturer go in using restrictions on access control technology to prevent competitors from legitimately using reverse engineering to develop competitive, interoperable noninfringing consumer goods?[13] This question, and the relationship between prohibitions on circumvention and the underlying law of copyright, makes the anticircumvention cases presently wending their way through the federal courts of interest to many.

**Lexmark International v. Static Control Components, Inc.** A U.S. district court granted Lexmark, a manufacturer of laser printers and printer toner cartridges, a preliminary injunction against a remanufacturer of replacement cartridges, Static Control Components (SCC), for copyright infringement and violation of § 1201 of the DMCA.

A toner cartridge is a device that is inserted within a laser printer and contains the toner necessary for the printer to print. Plaintiff Lexmark manufacturers two types of toner cartridges: a regular one that can be refilled by the printer owner or by a third party remanufacturer and a discounted one for its T-series printers which, pursuant to a licensing agreement, consumers agree to use only once and return to Lexmark for recycling. SCC and other remanufacturers refill and sell Lexmark's regular toner cartridges.

Lexmark employs copyrighted computer programs embedded within microchips to control and monitor various operations on the T-series toner cartridges. It utilizes an authentication sequence to prevent unauthorized access to its Printer Engine and Toner Loading Program (TLP). In the absence of the authentication sequence, a printer will not recognize a toner cartridge as being authorized and disables access to the Printer Engine Program.

Defendant SCC manufactures and sells components for use in the remanufacturing of toner cartridges. By reverse engineering the Lexmark microchip, SCC developed a microchip that copies, and thereby circumvents, the authentication sequence that Lexmark uses in the T-Series printers. This enables SCC to sell its "SMARTEK" microchip for use by third-parties to market replacement toner cartridges that are compatible with the T-series despite Lexmark's intention to limit replacement cartridges to those it manufactures.

*U.S. District Court.* Lexmark sued SCC in U.S. district court and received a preliminary injunction against the continuing sale by SCC of the "SMARTEK"

---

[12] Assessment Technologies of WI v. Wiredata, Inc., 350 F.3d 640, 647 (7th Cir. 2003).

[13] *See* Dan L. Burk, *Anticircumvention Misuse,* 50 U.C.L.A. L. REV. 1095, 1135 (2003). The author advocates development of a judicial doctrine of "anticircumvention misuse," akin to copyright misuse, to curb anticompetitive applications of access-control technology. "[A] finding of misuse would be proper where the ends to which the anticircumvention right is put exceed the reasonable grant of the right. For this standard to have any definite structure it will be necessary to determine what the bounds of the anticircumvention grant might be."

microchip for T-series replacement cartridges. The court found that Lexmark was likely to prevail on claims of copyright infringement and violation of the DMCA.[14]

There were two distinct components of SCC's microchip. One circumvented an authentication sequence embedded in the T-series printer. The sequence determines whether the printer will accept the cartridge as authorized and subsequently grant it access to the Printer Engine Program which is resident in the printer's controller board. The other both circumvented access to and copied Lexmark's TLP in its entirety. The Toner Loading Program enables the printers to approximate the amount of toner remaining in the cartridge. This information is used to display a "toner low" message on the printer screen.

The question before the court was twofold: First, did the SMARTEK microchip violate the DMCA by illegally circumventing the access control systems to both the Printer Engine Program and the Toner Loading Program? Second, by replicating the TLP in its entirety, did the microchip infringe Lexmark's copyright in it? The court considered in depth whether the Lexmark's Toner Program was copyrightable and concluded that it was, relying in part upon the fact that the U.S. Copyright Office granted Lexmark of a Certificate of Registration for it. It considered and rejected a fair use defense. It also rejected a copyright misuse defense, finding that attempting to enforce rights under the DMCA to protect access to a copyrighted computer program *cannot* have the legal effect of "using copyright to secure an exclusive right or limited monopoly not expressly granted by copyright law."[15]

Nor could Lexmark's efforts to enforce its rights under the DMCA be considered an unlawful act undertaken to stifle competition. The court emphasized that under the DMCA, "the right to protect against unauthorized access is a right separate and distinct from the right to protect against violations of exclusive copyright rights such as reproduction and distribution."[16] Indeed, the authentication sequence which triggered the interface between Lexmark's toner cartridge microchip and printer was exactly the type of "technological measure that effectively controls access to a work" designed to be protected under the DMCA.[17]

Finally, the court rejected the argument that the DMCA's exemption for reverse engineering was applicable to SCC's SMARTEK microchip.[18] In addition to

---

[14] 253 F.Supp.2d 943 (E.D.Ky. 2003), *rev'd*, 387 F.3d 522 (6th Cir. 2004).

[15] *See also* Sony Computer Entertainment America. Inc. v. Gamemasters, 87 F.Supp.2d 976 (N.D.Ca. 1999)(no copyright misuse where plaintiff sued to prevent defendant from selling counterfeit accessories which circumvented access controls on plaintiff's game console and CD-ROMs.)

[16] 253 F.Supp.2d at 969.

[17] *Id.* at 967.

[18] Sections 1201(f)(2) and (3) provide that a person may develop a circumvention device and make that circumvention device available to others "*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 under this title or violate*

(continued...)

violating the DMCA by circumventing the authentication sequence to the Printer Engine Program, SCC's microchip infringed the Copyright Act because it contained an exact copy of Lexmark's copyrighted Toner Loading Program. Therefore, SCC was unable to meet the reverse engineering exemption requirement that the circumvention enables interoperability of an *independently created* computer program.

*The Court of Appeals.* The Sixth Circuit Court of Appeals overturned the lower court's issuance of a preliminary injunction, taking issue with virtually all of the district court's findings.[19] Specifically, the Court of Appeals found that, for purposes of upholding a preliminary injunction, Lexmark was not likely to successfully establish that SCC infringed its copyright for the TLP or that the SMARTEK microchip violated the DMCA by illegally circumventing access controls.

The court first considered the TLP's eligibility for copyright protection. It weighed the basic element for copyrightability, original and/or creative expression, against that which *cannot* be copyrighted – an idea, procedure, process, system, method of operation, concept, principle or discovery, regardless of form.[20] Applying this process to computer programs with its concomitant task of separating idea from expression is "vexing."[21] In order to ascertain the "elusive boundary line" between idea/expression and between process/non-functional expression, the court utilized the doctrines of "merger" and "scènes à faire." The merger doctrine precludes copyright protection where there is only one way or very few ways of expressing an idea. Idea and expression are deemed to be merged because granting copyright to the expressive component of the work would extend protection to the work's uncopyrightable ideas as well. The scènes à faire doctrine is related. In the computer-software context it means

> that the elements of a program dictated by practical realities--*e.g.,* by hardware standards and mechanical specifications, software standards and compatibility requirements, computer manufacturer design standards, target industry practices, and standard computer programming practices--may not obtain [copyright] protection.[22]

The court noted that lock-out codes generally fall on the functional-idea rather than the original-expression side of the copyright line. Manufacturers of interoperable devices such as toner cartridges or garage door opener transmitters often employ a security system to bar the use of unauthorized components. To unlock the system to permit operation of the primary device, the printer or the garage door opener, the component must contain certain code or be engineered to respond

---

[18] (...continued)
*applicable law other than this section.*" 17 U.S.C. § 1201(f)(3) (emphasis added).

[19] 387 F.3d 522 (6th Cir. 2004).

[20] 17 U.S.C. § 102(b).

[21] 387 F.3d at 535.

[22] *Id.*

correctly to an authentication sequence. When a code sequence must be included in a component device to permit its use, the merger and scènes à faire doctrines often preclude the sequence from obtaining copyright protection.

Applying the foregoing, the court concluded that the district court erred in finding that the TLP code had sufficient originality to be copyrightable. It found the TLP to be a very brief, uncomplicated code sequence that functioned as a lock out code. Brevity in a computer program does not make it ineligible for copyright protection, but creativity and effort are reciprocally related: the smaller the effort, the greater the creativity required to invoke copyright protection.[23]

In view of its finding that the TLP was not copyrightable, the court declined to rule on SCC's fair use defense. It did, however, indicate that although the purpose of SCC's use of the SMARTEK chip was for commercial gain, a factor in a fair use analysis, its use of the copyrighted TLP on the chip was not. Rather, the use of the TLP was to satisfy authentication requirements and to permit printer functionality. Likewise, with respect to the allegedly infringing use on the value of the copyrighted work, the lower court had concluded that the SMARTEK chip would diminish the market for sales of Lexmark's toner cartridges. The proper and more narrow question, however, was whether replication of the TLP on the microchip would diminish demand for the TLP. More significantly, the Court of Appeals observed that copyright law is not properly invoked to protect a secondary market in consumer goods:

> [T]he district court focused on the wrong market: it focused not on the value or marketability of the Toner Loading Program, but on Lexmark's market for its toner cartridges. Lexmark's market for its toner cartridges and the profitability of its Prebate program may well be diminished by the SMARTEK chip, but that is not the sort of market or value that copyright law protects. ... Lexmark has not introduced any evidence showing that an independent market exists for a program as elementary as its Toner Loading Program, and we doubt at any rate that the SMARTEK chip could have displaced any value in *this* market.[24]

The Court of Appeals then addressed the district court's findings with respect to Lexmark's likelihood of success in establishing that SCC violated the DMCA's ban on distributing devices that circumvent access-control measures placed on copyrighted works. According to Lexmark, SCC's SMARTEK chip is a "device" that "circumvents" Lexmark's "technological measure," i.e., the authentication sequence, which "effectively controls access" to its copyrighted works (the Toner Loading Program and Printer Engine Program). Lexmark claimed that the SMARTEK chip met all three tests for liability under § 1201(a)(2): (1) the chip was "primarily designed or produced for the purpose of circumventing" Lexmark's authentication sequence, (2) it had "only limited commercially significant purpose or use other than to circumvent" the authentication sequence; and (3) SCC marketed the chip "for use in circumventing" the authentication sequence. The district court

---

[23] *Id.* at 543.

[24] *Id.* at 545. (Citation omitted; emphasis in original.)

agreed and concluded that Lexmark had shown a likelihood of success under all three provisions.

For the Court of Appeals, the anticircumvention allegation with respect to the TLP was problematic. The microchip did not provide "access" to the TLP but actually replaced it. More important, since the DMCA prohibits circumvention of access controls for *copyrighted* work, the determination that the TLP was not eligible for copyright protection mooted the DMCA charge.

The charge of illegal circumvention of the authentication sequence for the copyrighted Printer Engine Program was more complicated. The district court determined that the authentication sequence "controlled access" to the Printer Engine Program because it controlled the consumer's "ability to make use of" the program. The Court of Appeals disagreed, asserting that the authentication sequence did *not* control access, rather "[i]t is the purchase of a Lexmark printer that allows 'access' to the program."[25] The literal code itself can be read directly from the printer memory without the benefit of the authentication sequence. There is no security device protecting the Printer Engine Program. While the authentication sequence controls access to the Printer Engine Program's functionality, the Program itself is not otherwise effectively protected by access controls; the data and program can be translated into readable source code. Hence, the authentication sequence controlled only one avenue of access – operational compatibility with a printer cartridge. Analogizing access controls to locks on a house, the court reasoned:

> 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.[26]

The court elaborated by explaining why access to the Printer Engine Program is not covered by the DMCA. In the setting where the DMCA applies, such as encrypted data on music CDs and motion-picture DVDs, the copyright content that it protects operates on "two planes": the literal code governing the content and its manifestation generated by the code's execution, namely, the music or movie. In the DMCA's context, restricting "use" of the work means "restricting consumers from making use of the copyrightable expression in the work."[27] The manufacturer must prevent access to both planes of the copyrighted material and the alleged infringer responds by marketing a device that circumvents both levels of protection. Thus, because Lexmark did not direct any of its security efforts, through the authentication sequence or otherwise, to ensuring that the Printer Engine Program could not be read

---

[25] *Id.* at 546.

[26] *Id.* at 547.

[27] *Id.* at 548.

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].'"

The extent to which the court leaves open an invitation to manufacturers to come within the DMCA by withholding all levels of access to copyright-protected code is less clear. It refers to the act's legislative history and discerns congressional intent to protect the market for interoperable consumer goods, but nevertheless emphasizes its "two plane" analysis:

> 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. In fact, Congress added the interoperability provision in part to ensure that the DMCA would not diminish the benefit to consumers of interoperable devices "in the consumer electronics environment." 144 Cong. Rec. E2136 (daily ed. Oct. 13, 1998) (remarks of Rep. Bliley).[28]

Interestingly, in a concurring opinion, Circuit Judge Merritt addresses this very point. He advocates broadening the scope of the holding by making 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."[29]

In his opinion, the critical question is the purpose of the circumvention technology. Because the purpose of the law is to prohibit piracy of copyright protected works such as movies, music, and computer programs, an anticircumvention claim should not be permitted to go forward unless the plaintiff can demonstrate that the circumvention supports piracy. A broad reading of the statute is necessary, he argues, to prevent manufacturers from creating monopolies for durable goods such as replacement parts through the use of more elaborate lock out codes. And the burden of proof to demonstrate piracy must be on the plaintiff in order to prevent the threat of litigation by powerful manufacturers against smaller rivals and thereby thwart development of devices that facilitate legitimate access to consumer goods. Only then should the burden of proof shift to the defendant to invoke a statutory exception, such as the reverse engineering exception.

**Chamberlain Group, Inc. v. Skylink Technologies, Inc.** In three reported decisions, a U.S. district court and the Court of Appeals for the Federal Circuit considered the claim of plaintiff Chamberlain, a garage door opener (GDO) manufacturer, that defendant Skylink's universal remote control GDO transmitter violated the DMCA. Chamberlain manufactures and sells a variety of GDO systems. Its "Security+" line incorporates a copyrighted computer program known as its "rolling code" system to transmit changing signals. The rolling code system is designed to enhance the security of its GDO by preventing "code grabbers" from

---

[28] *Id.* at 549.

[29] *Id.* at 551.

intercepting the GDO signal. Skylink markets a universal remote transmitter, Model 39, which functions with a wide variety of GDOs. It does not incorporate Chamberlain's rolling code, but has one specific setting that operates the rolling code GDO. Chamberlain sued Skylink, asserting that the Model 39 transmitter is marketed for use in circumventing its rolling code computer program and that it renders the Security+ GDO insecure by allowing unauthorized users to circumvent the security inherent in the rolling code. Consequently, Chamberlain contended that Skylink violated the anti-trafficking clause of the DMCA's anticircumvention provision, § 1201(a)(2).

*U.S. District Court Holdings.* In the first of two reported U.S. district court decisions, the court considered whether Chamberlain's rolling code security system was protected by copyright and whether the DMCA applied.[30] The court in denying Chamberlain's motion for summary judgment established a framework for its anticircumvention analysis, noting that it is "undisputed" that the DMCA's application is not limited to the Internet.[31] It was specifically intended to prohibit the trafficking of products or devices that circumvent technological measures to restrict access to copyrighted work.

In the second opinion,[32] the court granted defendant Skylink's motion for summary judgment determining that the Model 39 transmitter did not provide *unauthorized* access to Chamberlain's copyrighted software. Skylink's program to overcome Chamberlain's rolling code did not satisfy the statutory definition of circumvention *without the authority of the copyright owner*.[33] The court did not require Skylink to prove that its use was authorized. Rather, the burden was on Chamberlain to demonstrate that the use was unauthorized. The court found the following criteria persuasive to support its conclusion that Skylink's use of the rolling code was authorized:

- Chamberlain did not put any restrictions on consumers regarding the type of transmitter they needed buy to operate its GDO;
- Chamberlain also marketed a universal transmitter and did not advise consumers that they were limited to purchasing replacements from Chamberlain; and
- In order for a Skylink transmitter to operate a Chamberlain GDO, the homeowner must store the transmitter's signal into the GDO's

---

[30] Chamberlain Group, Inc. v. Skylink Technologies, Inc., 292 F.Supp.2d 1023 (N.D.Ill. 2003) (*Chamberlain I*).

[31] *Id.* at 1035.

[32] Chamberlain Group, Inc. v. Skylink Technologies, Inc., 292 F.Supp.2d 1040 (N.D.Ill. 2003) (*Chamberlain II*), *aff'd* 381 F.3d 1178 (Fed. Cir. 2004).

[33] 17 U.S.C. § 1201(a)(3)(A) provides that to circumvent a technological measure "means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, by-pass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner[.]"

> memory. Hence, it is the consumer, not Skylink, that authorizes access.

Skylink's Model 39 universal GDO transmitter did not violate the statute because creating and marketing one that is interoperable with the Chamberlain GDO was implicitly authorized.

The court emphasized two factors: homeowner expectations and industry practice. In response to Chamberlain's argument that it never warned customers against using unauthorized transmitters because it had no idea that other transmitters could be made to operate its rolling code, the court replied that Chamberlain's failure to anticipate new technology "does not refute the fact that homeowners have a reasonable expectation of using the technology now that it is available."[34] The fact that there is "a history in the GDO industry of universal transmitters being marketed and sold to allow homeowners an alternative means to access any brand of GDO" negated Chamberlain's contention that there was an implied restriction against the use of competing transmitters.[35]

The court compared the absence of an explicit limitation by Chamberlain on the use of competing transmitters to Lexmark's explicit restrictions against use of third-party toner cartridge refills in its shrinkwrap agreement with consumers. Yet, while simultaneously acknowledging the limitations that may be effected by a shrinkwrap agreement, the court also suggested that "legitimate consumer expectations" may constitute an independent "fair use" basis for circumventing access control technology:

> [A] homeowner has a legitimate expectation that he or she will be able to access the garage even if the original transmitter is misplaced or malfunctions. .... Under Chamberlain's theory, any customer who loses his or her Chamberlain transmitter, but manages to operate the opener either with a non-Chamberlain transmitter or by some other means of circumventing the rolling code, has violated the DMCA. In this court's view, the statute does not require such a conclusion. GDO transmitters are similar to television remote controls in that consumers of both products may need to replace them at some point due to damage or loss, and may program them to work with other devices manufactured by different companies. In both cases, consumers have a reasonable expectation that they can replace the original product with a competing, universal product without violating federal law.[36]

The court assigned significant weight to two factors in issuing the summary judgment in favor of Skylink. First, that the process by which the Model 39 transmitter passed Chamberlain's rolling code was not created without authorization and, second, that the burden of proof to demonstrate the absence of authorization is on the party alleging violation of the anticircumvention statute. It therefore rejected Chamberlain's contention that Skylink violated the prima facie requirement of anti-

---

[34] 292 F.Supp.2d at 1044.

[35] *Id.* at 1045.

[36] *Id.* at 1046.

trafficking under § 1201(a)(2) because its transmitter bypasses Chamberlain's rolling code security measure to gain access to Chamberlain's copyrighted GDO receiver operating software.

*Court of Appeals.* The Court of Appeals noted that to determine whether Skylink was entitled to summary judgment on the grounds that its Model 39 universal transmitter does not violate the DMCA requires the statutory construction of what § 1201(a)(2) does prohibit, a matter of "first impression."[37] It reviewed proceedings before the lower court, emphasizing the significance of the fact that Chamberlain did *not* allege that Skylink had infringed its copyright or was liable for contributory copyright infringement. And, with respect to the question of *unauthorized* circumvention, the court reiterated that the homeowner who purchases a Chamberlain GDO owns it and has a right to access his or her garage with it. Chamberlain did not place any explicit terms or conditions to limit the ways a purchaser may use its products. The homeowner who wishes to use a Skylink transmitter to operate with the Chamberlain GDO must program it to do so. Hence, if Chamberlain's interpretation of the DMCA were correct, not only would Skylink be in violation of the DMCA for trafficking in circumvention devices under § 1201(a)(2), but owners of a Chamberlain GDO who purchased a Skylink transmitter would be in violation of (a)(1) which prohibits circumvention.[38]

But the Court of Appeals, departing from the lower court's analysis, undertook a more expansive interpretation of the anticircumvention statute and did not limit its examination to the question of "authorization" as a component of the statutory definition of circumvention. It began by examining the "essence"of § 1201 which, it found, does not create a new property right. Circumvention is not legally synonymous with infringement:

> 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.[39]

The distinction is evident in the basis for stating the claim. A plaintiff alleging copyright infringement need only prove ownership and copying to make a claim. The burden of proving that the use was authorized falls on the defendant. But a plaintiff alleging illegal circumvention or trafficking must prove that the defendant's access was unauthorized, a significant burden of proof which requires the plaintiff to establish that copyright law does *not* permit the access. Only then does the burden shift to the defendant.

---

[37] 381 F.3d 1178, 1185, 1191 (Fed. Cir. 2004). The court distinguished the case before it from Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001), which focused on First Amendment issues in relation to the DMCA's anticircumvention provisions.

[38] 381 F.3d at 1187.

[39] *Id.* at 1192-93.

The court rejected Chamberlain's argument that enactment of the DMCA renders pre-DMCA history in the GDO industry "irrelevant" and overrides pre-existing consumer expectations about the legitimate uses of products containing copyrighted-embedded software. It rejected the broader contention that, in the absence of explicit authorization, circumvention of any technological access control measure to use a product containing copyrighted software is *per se* illegal. To subscribe to such an interpretation of the statute would grant manufacturers "broad exemptions from both the antitrust laws and the doctrine of copyright misuse."[40]

In other words, the DMCA's prohibition against circumvention does create a new and independent cause of action separate from copyright infringement.[41] But in order to establish liability for unauthorized circumvention, the complainant must demonstrate that access is indeed linked to copyright infringement. And this linkage allows the court to consider all non-infringing uses, including statutorily and judicially established fair uses. Hence, to violate the DMCA by circumventing access technology "without the authority of the copyright owner" means to circumvent *for a purpose impermissible under the copyright laws*; not simply to circumvent without the express permission of the copyright owner.[42]

The court examined § 1201's construction and legislative history and determined that the key to disentangling these relationships lies in understanding the linkage between "access" and "protection." Tying prohibitions against access to protectible rights under copyright law represents a "rebalancing of interests" that addresses digital piracy. Granting copyright owners unqualified control over technological access would create "two distinct copyright regimes." The first regime permits copyright owners to protect only the rights enumerated in 17 U.S.C. § 106, subject to the exceptions and limitations of the Copyright Act. Owners who attempt to protect their rights by incorporating technological measures to protect against encroachment are able to hold traffickers in circumvention devices liable under § 1201(b) for putting their rights at risk by enabling users of the devices *to infringe*.

Under the second regime – inherent in Chamberlain's argument and rejected by the court – the owners of a work protected by both copyright *and* a technological measure that controls access to that work would possess *unlimited* rights to hold circumventors liable under 1201(a) simply for accessing that work, even if that access enabled *only* rights that the Copyright Act grants to the public. This interpretation, even under the "substantial deference due Congress ... borders on the irrational."[43]

---

[40] *Id.* at 1193.

[41] "Circumvention is not a new form of infringement but rather a new violation prohibiting actions or products that facilitate infringement[.]" *Id.* at 1197.

[42] This interpretation, the court noted, helps 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." *Id.* at 1194.

[43] *Id.* at 1200.

Addressing concerns of many DMCA critics, the court explained that the doctrines of antitrust and copyright misuse are inescapable components of a right to control technological access to copyrighted work:

> 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.[44]

Indeed, even if the grant to prohibit circumvention were a property right, it would still not serve to repeal by implication the rights of those who lawfully possess copyrighted property. If lawful ownership of encryption-protected property conferred two separate and distinct rights on the copyright holder, the latter would be empowered to prohibit lawful access to the copyrighted content. In the instant case, the owner of a Chamberlain GDO has a legal right, that is, a fair use right under copyright law, to use a universal transmitter manufactured by a third-party to access the copyrighted software to open the garage door:

> 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.[45]

While the DMCA granted copyright holders additional legal protection, it did not rescind the basic bargain granting the public noninfringing and fair uses of copyrighted materials. The act also permits the various express beneficial uses of circumvention technology, such as those exempted under § 1201(d),(f),(g), and (j) from the anticircumvention ban.

The court held 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 owners. It speculated that its holding might "create some uncertainty and consume some judicial resources," but nevertheless concluded that it is the only meaningful reading of the statute.

---

[44] *Id.* at 1201. (Citations and footnote omitted.)

[45] *Id.* at 1202. (Footnote omitted)(Emphasis in original).

Building upon its assumptions, the court articulated a very specific test to determine what a plaintiff alleging a violation of § 1201(a)(2) trafficking must establish:

> 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.[46]

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, Chamberlain established no connection between unauthorized use of its copyrighted software and Skylink's accused transmitter. Hence, the court affirmed the district court's grant of summary judgment to Skylink.

**Conclusion.** The major challenges presented by both the *Lexmark* and *Chamberlain* cases are to define the relationships between and effects of the anticircumvention restrictions on reverse engineering, in particular, and underlying principles of copyright law, in general. These cases represent the application of anticircumvention principles to access control technology in a broader market of consumer goods. In both cases, a Court of Appeals read the restrictions on circumvention more narrowly than the interpretation asserted by the plaintiff, placing the initial burden on the plaintiff to establish not just the fact of circumvention, but its wrongfulness as well. In both cases, the courts strove to reconcile existing copyright law principles of fair use with the newer, independent constraints on circumvention. While these decisions may allay some of the DMCA's critics' concerns regarding anticircumvention and fair use, the facts before the courts ensures that they cannot define the outer limits for the use of access control technology as a means to assert control over durable goods.

---

[46] *Id.* at 1203. (Emphasis in original).