

GARAGE DOOR OPENERS, PRINTER TONER CARTRIDGES, AND THE NEW AGE OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

*Caryn C. Borg-Breen**

I.	INTRODUCTION.....	885
II.	THE DMCA AND ITS APPLICATION TO DURABLE GOODS.....	889
	A. <i>Background of the DMCA and Its Provisions</i>	889
	B. <i>The DMCA and Garage Door Openers</i>	895
	C. <i>The DMCA and Toner Printer Cartridges</i>	897
III.	ANALYSIS OF THE DMCA.....	898
	A. <i>The Federal Circuit's Ruling in Chamberlain Group v. Skylink Technologies</i>	899
	B. <i>The Sixth Circuit's Ruling in Lexmark v. Static Control Components</i>	903
	C. <i>Analyzing the DMCA in View of Chamberlain and Lexmark</i>	905
	D. <i>Conclusion Regarding Courts' Interpretations</i>	912
IV.	EVALUATION OF THE CHAMBERLAIN TEST.....	912
	A. <i>Chamberlain Test Applied to Lexmark v. Static Control</i>	913
	B. <i>Chamberlain Test Applied to Sony v. Gamemasters</i>	915
	C. <i>Chamberlain Test Applied to Davidson v. Internet Gateway</i>	918
V.	THE FUTURE OF THE DMCA.....	922
VI.	CONCLUSION.....	924

I. INTRODUCTION

Since its enactment, the Digital Millennium Copyright Act (“DMCA”) of 1998,¹ and in particular its anticircumvention and antitrafficking provisions, has been the subject of extensive debate.² The DMCA created new liability for circumvention of technological protection measures used by

* J.D. Candidate, Northwestern University School of Law, 2006; Ph.D., Chemistry, University of North Carolina at Chapel Hill; B.S., Chemistry, College of William and Mary.

¹ Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998). The Act is currently incorporated into chapter 12 of Title 17 of the United States Code, most notably, for purposes of this Comment, §§ 1201 to 1205. See 17 U.S.C. §§ 1201–1205 (2000).

² A WestLaw search returns well over 2000 law review articles mentioning the DMCA with over 160 mentioning the Act in the title.

copyright owners to control access to their works.³ The DMCA provisions created liability for the act of circumventing a DVD encryption program as well as for selling a DVD player with built-in decryption software, even when neither act was in and of itself a violation of copyright law. Critics have debated the proper construction of the text of the DMCA. In particular, consumer rights groups have warned that, if the DMCA were broadly construed so “circumvention” is completely divorced from any act of copyright infringement, the law would protect not only “digital content products”—such as DVD movies and video games⁴—but also any product affixed with an electronic lock that incorporated a few bytes of copyrighted computer code. Such a broad construction would extend a copyright monopoly to the underlying uncopyrightable products.⁵ The initial cases testing the DMCA provisions all involved digital content products—the very types of cases Congress intended the DMCA to address.⁶

When two large durable goods manufacturers,⁷ Chamberlain Group and Lexmark International, asserted claims under the DMCA—Chamberlain’s involving after-market⁸ garage door openers and Lexmark’s involving a toner printer cartridge designed to circumvent electronic locks

³ See *infra* notes 35–50 and accompanying text (discussing the provisions of the DMCA).

⁴ Examples of digital content products include DVD movies, video games, music files, and e-books. See Daniel C. Higgs, *Lexmark International, Inc. v. Static Control Components, Inc. & Chamberlain Group, Inc. v. Skylink Technologies, Inc.: The DMCA and Durable Goods AfterMarkets*, 19 BERKELEY TECH. L.J. 59, 67 (2004).

⁵ See, e.g., Jane C. Ginsburg, *Copyright Legislation for the “Digital Millennium,”* 23 COLUM.-VLA J.L. & ARTS 137 (1999); Daniel S. Hurwitz, *A Proposal in Hindsight: Restoring Copyright’s Delicate Balance by Reworking 17 U.S.C. § 1201*, 2005 UCLA J.L. & TECH. 1; Paul R. Kitch, *DMCA is OEMs Ticket to “Super-Patenting” the Unpatentable*, INTELL. PROP. & TECH. L.J., March 2005, at 5; David Nimmer, *Codifying Copyright Comprehensibly*, 51 UCLA L. REV. 1233, 1342 (2004) [hereinafter Nimmer, *Codifying Copyright Comprehensibility*] (calling the DMCA “the granddaddy of all distensions of copyright doctrine, reminiscent of Jeremy Bentham’s ‘nonsense on stilts’”); David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673 (2000) [hereinafter Nimmer, *A Riff on Fair Use*]; Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999); Yijun Tian, *Problems of Anti-Circumvention Rules in the DMCA & More Heterogeneous Solutions*, 15 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 749 (2005); Pete Singer, Comment, *Mounting a Fair Use Defense to the Anti-Circumvention Provisions of the Digital Millennium Copyright Act*, 28 U. DAYTON L. REV. 111 (2002); Elec. Frontier Found., *Unintended Consequences: Five Years Under the DMCA*, EFF.ORG, Sept. 24, 2003, http://www.eff.org/IP/DMCA/unintended_consequences.pdf.

⁶ See, e.g., *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002) (eBook reader); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (encrypted movies); *RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000) (streaming video); *Sony Computer Entm’t Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976 (N.D. Cal. 1999) (video games).

⁷ “Durable goods” are products whose value is independent of any copyrighted material they contain. See Higgs, *supra* note 4, at 67. Durable goods manufacturers are also referred to as “original equipment manufacturers” (“OEMs”). See Kitch, *supra* note 5.

⁸ “After-market” products are parts or accessories used in the upkeep or enhancement of a previous purchase. Replacement oil filters for cars, for example, constitute after-market products.

containing copyrighted computer programs—critics’ fears that the DMCA would be improperly applied outside the digital content products arena appeared warranted.⁹ The district courts considering this new challenge under the DMCA gave conflicting rulings: Chamberlain Group’s DMCA claim was dismissed by the Northern District of Illinois in *Chamberlain Group, Inc. v. Skylink Technologies, Inc. (Chamberlain I & II)*,¹⁰ while the Eastern District of Kentucky upheld the DMCA claim in *Lexmark International, Inc. v. Static Control Components (Lexmark I)*.¹¹ Not surprisingly, both cases were appealed. Until these appeals, no appellate court had considered a case that fully tested the limits of the DMCA (with respect to either digital content products or durable goods) and, accordingly, no appellate court had been forced to decide where to draw the line for liability.¹² The Federal Circuit, in *Chamberlain III*,¹³ was the first of the appellate courts to render its decision, and the Sixth Circuit’s decision in *Lexmark II*¹⁴ followed just two months later.

In a victory for consumer rights groups, the Federal Circuit in *Chamberlain III* held in favor of after-market competition and boldly declared that a broad, plain-meaning construction of the DMCA was “absurd.”¹⁵ Specifically, the court interpreted the DMCA provisions to require a “reasonable relation” between the act of circumvention and infringement of a copyrighted work (although it did not go so far as to require actual infringement).¹⁶ The Federal Circuit’s interpretation is significant in two respects. First, the court’s interpretation excludes from liability users or traffickers of devices that circumvent encryption codes or electronic locks in ways that do not facilitate copyright infringement. For example, under the court’s interpretation, a durable goods manufacturer cannot use the DMCA to prevent competitors from circumventing a copyright-protected “electronic lock” attached to after-market goods. The Federal Circuit’s decision is also significant because it lays out a six-part test for DMCA liabil-

⁹ See *Lexmark Int’l, Inc. v. Static Control Components, Inc. (Lexmark I)*, 253 F. Supp. 2d 943 (E.D. Ky. 2003); *Chamberlain Group, Inc. v. Skylink Techs., Inc. (Chamberlain I)*, 292 F. Supp. 2d 1023 (N.D. Ill. 2003); *Chamberlain Group, Inc. v. Skylink Techs. (Chamberlain II), Inc.*, 292 F. Supp. 2d 1040 (N.D. Ill. 2003).

¹⁰ *Chamberlain I*, 292 F. Supp. 2d at 1023.

¹¹ *Lexmark I*, 253 F. Supp. 2d at 943.

¹² The Second Circuit has previously considered the constitutionality of § 1201(a)(2) under the First Amendment. See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

¹³ *Chamberlain Group, Inc. v. Skylink Techs., Inc. (Chamberlain III)*, 381 F.3d 1178 (Fed. Cir. 2004).

¹⁴ 387 F.3d 522 (6th Cir. 2004).

¹⁵ *Chamberlain III*, 381 F.3d. at 1201. The appeal from the Northern District of Illinois went to the Federal Circuit instead of the Seventh Circuit because the case also involved a patent claim, for which the Federal Circuit has appellate jurisdiction under 28 U.S.C § 1295(a)(1) (2000). As discussed *infra* note 98, the Federal Circuit’s assertion of jurisdiction is questionable since the patent claim was dismissed by the trial court without prejudice prior to appeal.

¹⁶ *Chamberlain III*, 381 F.3d at 1202.

ity, which includes an element requiring that the act of circumvention facilitate copyright infringement.¹⁷ Thus, the Federal Circuit's new test narrows the scope of liability under the DMCA while providing a workable framework for determining liability under the DMCA.

While the Second Circuit had previously considered a constitutional challenge to the DMCA,¹⁸ the Federal Circuit's decision in *Chamberlain III* marks the first time an appellate court has addressed the liabilities created by the anticircumvention and antitrafficking provisions of the DMCA.¹⁹ Soon after, the Sixth Circuit overturned the district court verdict in *Lexmark II*²⁰ and similarly rejected a broad construction of the DMCA.²¹ Despite reaching the same conclusion regarding liability, the Federal Circuit and Sixth Circuit took markedly different approaches to analyzing the DMCA.²² In particular, the Federal Circuit in *Chamberlain III* found there was no DMCA violation because there was no nexus between the act of circumvention and copyright infringement,²³ whereas the Sixth Circuit in *Lexmark II* found there was no violation because the copyrighted program could be accessed without circumventing the access control measure.²⁴

Although these appellate court decisions provide a glimmer of insight into the bounds of the anticircumvention and antitrafficking provisions, many questions still remain as to whether the Federal and Sixth Circuits' interpretation of those provisions is limiting enough to allay the fears highlighted by consumer rights advocates.²⁵ What are the implications of the Court's interpretation of the DMCA in *Chamberlain III*? Was the court justified in disposing of the plain meaning of the statutory text in favor of embracing policy arguments regarding application of the DMCA?

This Comment will address four topics. Part II provides some background on the DMCA provisions and how they were applied to garage door openers and printer toner cartridges in *Chamberlain* and *Lexmark*, respectively. Part III analyzes the reasoning used by the appellate courts to interpret provisions of the DMCA in *Chamberlain III* and *Lexmark II*. Part IV

¹⁷ *Id.* at 1203.

¹⁸ *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

¹⁹ *Chamberlain III*, 381 F.3d at 1178.

²⁰ 387 F.3d 522 (6th Cir. 2004).

²¹ *Id.* at 546–47.

²² *Id.*

²³ See *infra* note 136 and accompanying text.

²⁴ See *infra* notes 138–141 and accompanying text.

²⁵ The initial reaction to the *Chamberlain* decision has been cautiously optimistic. See, e.g., Steven Andersen, *Court Closes the Door on Chamberlain's DMCA Case: Federal Circuit's Decision Clarifies Overly Broad Statute*, CORP. LEGAL TIMES, Nov. 2004, at 16 (discussing how the decision put a limit on the scope of the DMCA); Jonathan Band, *How to Temper the Excesses of the DMCA*, LEGAL TIMES, Oct. 11, 2004, at 20, 21 (calling the Federal Circuit's decision in *Chamberlain* "The Right Decision"); Posting of Yip Yu to Copyfutures Weblog, http://lsolum.typepad.com/copyfutures/2004/09/a_step_in_the_r.html (Sept. 3, 2004, 08:24 PST).

focuses upon the Federal Circuit's "reasonable relationship test" and demonstrates that this test is workable and, if properly applied, will consistently result in a proper balance between the rights of the general public and the rights of copyright owners. Finally, Part V addresses some important DMCA issues left unresolved by the court's opinion in *Chamberlain III*.

II. THE DMCA AND ITS APPLICATION TO DURABLE GOODS

A. Background of the DMCA and Its Provisions

That the DMCA would be applied to durable goods was not contemplated at the time of its passage. The impetus for the DMCA arose from the content industries, including movie studios, book publishers, software developers, and music companies who persistently lobbied Congress, arguing that digital technology made large-scale and high-quality copying of copyrighted material easy and inexpensive. Representatives from these industries contended that the Copyright Act alone was insufficient to prevent hackers from circumventing electronic access controls and copying copyright-protected digital works.²⁶ In 1997, the World Intellectual Property Organization ("WIPO") Copyright Treaty was adopted, banning the circumvention of technological measures and the sale of circumvention devices.²⁷ The WIPO Copyright Treaty required contracting parties to

provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.²⁸

Congress enacted the DMCA a year later to implement the treaty and to bring "U.S. copyright law squarely into the digital age."²⁹

²⁶ See Higgs, *supra* note 4, at 59; Nimmer, *A Riff on Fair Use*, *supra* note 5; see also, Peter Moore, *Steal This Disk: Copy Protection, Consumers' Rights, and the Digital Millennium Copyright Act*, 97 NW. U. L. REV. 1437, 1438-39 (2003) (discussing problems with protecting copyrights in the wake of digital technology). As early as 1993, the Information Infrastructure Task Force established the Working Group on Intellectual Property Rights to hold a public hearing and evaluate changes to be made to copyright law. In 1995, the Working Group issued a White Paper containing recommendations, which were incorporated into a bill proposed by Senators Hatch and Leahy. This bill later became the basis for the DMCA. See S. REP. No. 105-190, at 2 (1998).

²⁷ Jeff White, *From Balance to Property: The Dangers of Copywrongs*, 6 TUL. J. TECH. & INTELL. PROP. 247, 257-58 (2004).

²⁸ WIPO Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-12, 36 I.L.M. 65 (1997), available at <http://www.wipo.int/documents/en/diplconf/distrib/94dc.htm>.

²⁹ S. REP. No. 105-190, at 2; H.R. Rep. No. 105-551, pt. 2, at 26 (1998) (noting that the purpose of the DMCA was to implement the "Copyright Treaty," and the "Performances and Phonograms Treaty" signed by the United States before the World Intellectual Property Organization). *But see* Samuelson, *supra* note 5, at 521 (arguing that the DMCA was unnecessary since U.S. law already complied with all

Congress hoped the DMCA would restore to copyright owners the technological and economic protections that were being threatened by advances in digital technology and the growth of electronic commerce.³⁰ Specifically, Congress acknowledged that without protection against massive piracy, copyright owners would be hesitant to make their works readily available in electronic commerce.³¹ The DMCA was intended to provide the needed protection and function as the “legal platform for launching the global digital on-line marketplace for copyrighted works.”³² The legislative history focused exclusively on the use of the DMCA to provide protection for digital content products in the stream of electronic commerce. The Senate Committee Report concluded, “[W]ith the DMCA, the Senate Judiciary Committee takes another important step toward protecting American ingenuity and creative expression.”³³ No mention was ever made of the applicability of the DMCA to durable goods. Further, no durable goods manufacturers participated in the hearings leading up to the enactment of the DMCA.³⁴

The DMCA contains three liability provisions: one anticircumvention provision³⁵ and two antitrafficking provisions.³⁶ The lone anticircumvention provision, § 1201(a)(1)(A), prohibits circumventing a technological measure that “effectively controls access to a work protected [by copyright].”³⁷ The corresponding antitrafficking provision, § 1201(a)(2), prohibits trafficking in a device whose purpose is to circumvent a technological measure that “effectively controls access” to a copyrighted work.³⁸ Both provisions of § 1201(a) generally relate to “access control measures.” Examples of access control measures include password protection, satellite

but one minor provision of the treaty and that the DMCA went far beyond the requirements of the treaty).

³⁰ H.R. REP. No. 105-551, pt. 2, at 2526 (“[T]he Committee also recognizes that the digital environment poses a unique threat to the rights of copyright owners, and as such, necessitates protection against devices that undermine copyright interests.”).

³¹ S. REP. No. 105-190, at 8.

³² *Id.*

³³ *Id.* at 69.

³⁴ See, e.g., S. REP. No. 105-190, at 3–4 (listing parties that participated in the Senate Committee hearings).

³⁵ 17 U.S.C. § 1201(a)(1)(A) (2000).

³⁶ *Id.* § 1201(a)(2)–(b)(1).

³⁷ *Id.* § 1201(a)(1)(A) (emphasis added).

³⁸ Specifically, the anticircumvention provision of the DMCA states:

No person shall manufacture, import, 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 this title; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that *effectively controls access* to a work protected under this title; or (C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing a technological measure that *effectively controls access* to a work protected under this title.

Id. § 1201(a)(2) (emphasis added).

scrambling, and measures that restrict a person from viewing a DVD movie outside of a twenty-four-hour period.³⁹

Congress considered the act of circumvention recited in § 1201(a) to be the “electronic equivalent of breaking into a locked room in order to obtain a copy of a book.”⁴⁰ However, nothing in the statutory language requires the access gained through circumvention to be connected to the act of copyright infringement. Moreover, neither the anticircumvention nor the anti-trafficking provisions define the term “access.” As a result, the statutory language could equally apply to breaking into a locked room in order to make a copy of a book—as envisioned by Congress—and to breaking into a locked room in order to obtain the book and using it to squash a bug.

Unlike the provisions in § 1201(a), § 1201(b), the second antitrafficking provision of the DMCA, generally relates to “rights control measures.” Specifically, § 1201(b)(1) prohibits trafficking in a device whose purpose is to circumvent protection afforded by a technological measure that “effectively protects a *right* of a copyright owner.”⁴¹ Such copyright owner rights include reproduction, distribution, adaptation, public performance, and public display rights.⁴² An example of a “rights control measure” is a measure that causes digital content to substantially degrade in quality in any copy made of the digital content, or a measure that prevents the making of copies at all.⁴³ In some devices, the access and rights control measures are merged into a single control measure.⁴⁴ For example, “Content Scramble System” (“CSS”) encryption, used for DVD movies, controls *access* because only a CSS-compliant player will allow the movie to be played; the CSS-compliant DVD player controls *rights* because a CSS-compliant DVD player will only allow a DVD movie to be viewed and not copied.⁴⁵

³⁹ See June M. Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts*, 27 COLUM. J.L. & ARTS 385, 450 (2004); R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH. L.J. 619, 625 (2003).

⁴⁰ H.R. REP. NO. 105-551, pt. 1, at 17 (1998).

⁴¹ The antitrafficking provision of the DMCA states:

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

17 U.S.C. § 1201(b)(1) (emphasis added).

⁴² 17 U.S.C. § 106.

⁴³ Besek, *supra* note 39, at 450.

⁴⁴ Reese, *supra* note 39, at 641–43.

⁴⁵ *Id.*

All three provisions create new civil⁴⁶ and, in some cases, criminal⁴⁷ liability. Significantly, the anticircumvention and antitrafficking provisions create liability even where there is no actual copyright infringement.⁴⁸ Also noteworthy is that the trafficker of a device that circumvents a rights control measure is liable under § 1201(b)(1) of the DMCA, whereas the actual circumventor of the rights control measure does not violate § 1201 (because the DMCA does not contain a rights control provision to parallel § 1201(a)(1)(A)) and therefore is not subject to remedies or penalties under §§ 1203 and 1204.⁴⁹ The DMCA also contains a series of limited exemptions from liability, including exemptions for encryption research, for reverse engineering when used for the purpose of interoperability, and for certain classes of activity that have been identified by the Librarian of Congress.⁵⁰

Considering the challenges inherent in crafting any statutory text and the complexity of digital technology, it is perhaps not surprising that the anticircumvention and antitrafficking provisions of the DMCA have come under significant scrutiny and criticism. Criticism of the DMCA provisions falls into three main categories. First, critics have questioned the constitutionality of the DMCA provisions in view of both the Intellectual Property Clause⁵¹ and the First Amendment. With respect to the Intellectual Property Clause, critics argue that the DMCA fails to “promote the progress of science and the useful arts” because the fear of criminal liability under the statute will cause researchers, particularly in the fields of computer security and cryptography, to discontinue their research or refrain from publishing their findings.⁵² This concern was borne out in the case of Princeton Com-

⁴⁶ 17 U.S.C. § 1203 (creating civil remedies including actual or statutory damages for violations of either § 1201 or 1202).

⁴⁷ 17 U.S.C. § 1204 (creating criminal remedies including fines up to \$500,000 and up to five years prison time if the circumvention is done “willfully and for purposes of commercial advantage or private financial gain”).

⁴⁸ Reese, *supra* note 39, at 626.

⁴⁹ A person who circumvents a rights control measure is still subject to liability for copyright infringement under 17 U.S.C. § 501(a). See Reese, *supra* note 39, at 623 (discussing how access controls and rights controls offer different legal protections).

⁵⁰ Reverse engineering is the general process of analyzing a technology specifically to ascertain how it was designed or how it operates. Interoperability allows technologies such as computer hardware, software, or both to work together when they use the same inputs and create the same outputs. For a detailed discussion of the DMCA’s exemptions, see, for example, Ginsburg, *supra* note 5, at 148–52; Nimmer, *A Riff on Fair Use*, *supra* note 5 at 692–99; Samuelson, *supra* note 5, at 537 (arguing that the exemptions address only the gravest concerns and are still too narrowly crafted).

⁵¹ Article I of the Constitution provides that Congress shall have the power “to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.” U.S. CONST. art. I, § 8, cl. 8.

⁵² See Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 SCIENCE 2028, 2028 (2001) (warning computer scientists that the DMCA could be used to prevent them from publishing their research); see also Kristin Brown, Comment, *Digital Rights Management: Trafficking in Technology*

puter Science Professor Ed Felten, who chose to refrain from publishing his research exposing weaknesses in a new digital watermarking technology when threatened with litigation under the DMCA by two music industry groups.⁵³ In addition, critics argue the DMCA violates the “limited times” grant of the Intellectual Property Clause by allowing copyright holders to use technological measures to extend their monopoly indefinitely.⁵⁴

With respect to the First Amendment, critics contend that code-breaking software, and the sale or publication thereof, is protected speech and that the DMCA is unconstitutionally vague, constituting a content-based restriction on speech that is not sufficiently narrowly tailored to serve the government’s interest.⁵⁵ Despite the criticisms, the constitutionality of the DMCA provisions under both the Intellectual Property Clause and the First Amendment has been challenged and upheld several times.⁵⁶

Second, critics argue that the DMCA provisions could be used to override exemptions from liability for fair use⁵⁷ of copyright protected works for

That Can Be Used to Circumvent the Intellectual Property Clause, 40 HOUS. L. REV. 803, 822 (2003) (discussing the chilling effect of the DMCA on scientific research).

⁵³ Secure Digital Music Initiative (“SDMI”), a group created by the Recording Industry Association of America (“RIAA”), issued a public challenge to computer scientists to try to defeat a digital watermarking technology, even offering a \$10,000 reward. When Professor Felten discovered weaknesses in the digital watermark and attempted to publish his research conclusions, SDMI and RIAA threatened to sue Professor Felten under the DMCA. The RIAA and SDMI warned Felten that his research publication would enable others to circumvent the technological measures used to prevent people from corrupting their copyright-protected watermarking technology and so would violate the DMCA antitrafficking provisions. Rather than face the high costs of litigation, Professor Felten withdrew his manuscript from publication. See Samuelson, *supra* note 52, at 2028–29.

⁵⁴ See Brown, *supra* note 52, at 813, 826–33 (discussing *Universal City Studios, Inc. v. Corley* and *United States v. Elcom Ltd.*, two cases involving a challenge to the constitutionality of the DMCA under the “limited times” provision of section 8 of Article I).

⁵⁵ See Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 420–22 (1999); John R. Therien, *Exorcising the Specter of a “Pay-Per-Use” Society: Toward Preserving Fair Use and the Public Domain in the Digital Age*, 16 BERKELEY TECH. L.J. 979, 1007–28 (2001).

⁵⁶ See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001) (holding that a DVD decryption computer program qualified as “speech” but that the injunction which prohibited Corley from publishing the decryption program on a website in violation of the antitrafficking provision of the DMCA was a content-neutral restriction on Corley’s speech and did not burden more speech than was necessary); *Edelman v. N2H2, Inc.*, 263 F. Supp. 2d 137 (D. Mass. 2003) (granting motion to dismiss plaintiff’s claim of First Amendment right to reverse engineer defendant software manufacturer’s internet blocking software and to publish the results without violating the antitrafficking provisions of the DMCA for lack of injury in fact); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002) (denying defendant’s motion to dismiss an indictment alleging that its sale of a computer program that allowed users to remove restrictions from Adobe Acrobat PDF files was a violation of the DMCA’s antitrafficking provisions on basis that the DMCA restriction on speech was content based, and not sufficiently tailored to serve a governmental interest); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

⁵⁷ Fair use is codified in the Copyright Act and provides an exception to copyright infringement “for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.” 17 U.S.C. § 107.

noncommercial purposes (such as educational uses) and for reverse engineering related to interoperability.⁵⁸ Although the DMCA states that “nothing in Section 1201 shall affect rights, remedies, limitations, or defense to copyright infringement, including fair use,”⁵⁹ the act does not expressly recognize users’ rights set forth in 17 U.S.C. §§ 107-122 of the Copyright Act, including fair use and first-sale rights.⁶⁰ Several courts have suggested that the scope of permitted uses under the DMCA is narrower than “fair use” as defined by the Copyright Act.⁶¹

Third, critics worry that although the DMCA was enacted to control electronic media piracy, it could be construed broadly and misused by durable goods manufacturers to improperly extend their monopoly to the after-market by including a copyrighted electronic lock on their products.⁶² For example, automobile manufacturers could incorporate microchips containing copyrighted software into their cars that would lock out unauthorized replacement parts such as brake shoes and oil filters.⁶³ Were a third party to design a device to side-step or disable the oil filter’s microchip and enable its own replacement filter to be used instead, liability under the DMCA could very well ensue.⁶⁴ Fears that the DMCA would be used to establish after-market monopolies appeared warranted when durable goods manufacturers Chamberlain Group and Lexmark International filed suits in district court alleging violations of the DMCA’s antitrafficking provision.⁶⁵

⁵⁸ See Carla Meninsky, *Locked Out: The New Hazards of Reverse Engineering*, 21 J. MARSHALL J. COMPUTER & INFO. L. 591 (2003); Nimmer, *A Riff on Fair Use*, *supra* note 5; Andrew Sparkler, *Senators, Congressmen, Please Heed the Call: Ensuring the Advancement of Digital Technology Through the Twenty-First Century*, 14 FORDHAM INTEL. PROP. MEDIA & ENT. L.J. 1137 (2004) White, *supra* note 27; see also Reese, *supra* note 39, at 629–31 (discussing the fact that § 1201(b)(2) does not require that rights control measures *only* protect rights of the copyright holder but may include control of noninfringing uses as well).

⁵⁹ 17 U.S.C. § 1201(c)(1).

⁶⁰ Some argue that fair use is constitutionally required. See Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 47 (2001). *But see* Matthew Sag, *God in the Machine: A New Structural Analysis of Copyright’s Fair Use Doctrine*, 11 MICH. TELECOMM. & TECH. L. REV. 381 (2005).

⁶¹ See *Corley*, 273 F.3d at 459 (“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.”); *Elcom*, 203 F. Supp. 2d at 1131.

⁶² See Brief for Consumers Union as Amicus Curiae Supporting Respondents, *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 292 F. Supp. 2d 1023 (N.D. Ill. 2003) (No. 02 C 6376); Meninsky, *supra* note 58; James D. Nguyen, *Code Breaking*, 27 L.A. LAW, May 2004, at 33, 41–42 (warning that “any media hardware that contains electronic parts or even a small amount of software can be embedded with technological protections to trigger the anticircumvention provisions”).

⁶³ Higgs, *supra* note 4, at 77.

⁶⁴ See generally Meninsky, *supra* note 58.

⁶⁵ See *Chamberlain I*, 292 F. Supp. 2d 1023; *Chamberlain II*, 292 F. Supp. 2d 1040 (N.D. Ill. 2003); *Lexmark I*, 253 F. Supp. 2d 943 (E.D. Ky. 2003).

B. *The DMCA and Garage Door Openers*

In *Chamberlain I*, the plaintiff, a manufacturer of garage door openers (“GDOs”), brought suit under the DMCA to enjoin Skylink from selling its after-market universal GDO transmitter.⁶⁶ A typical GDO contains a transmitter and receiver, which are set to recognize a unique transmitter “code.”⁶⁷ In order to prevent burglars from being able to “grab” the unique code by intercepting the signal, the Chamberlain GDO employed a “rolling code” technology whereby a copyrighted computer program constantly changed the radio frequency of the transmitter signal (the rolling code) required to activate the garage door motor.⁶⁸ The computer program served two functions: (1) to verify the rolling code sent from the transmitter (thus functioning as an access control measure) and (2) to activate the garage door motor once the correct rolling code was received.⁶⁹ The defendant’s after-market transmitter did not use rolling code technology; rather it was designed to transmit three fixed codes in rapid succession, causing the GDO to resynchronize and recognize one of the successive fixed codes.⁷⁰ In this way, the defendant’s transmitter could operate the Chamberlain GDO system.⁷¹

Chamberlain alleged that Skylink was prima facie liable for violating § 1201(a)(2) of the DMCA,⁷² which prohibits trafficking in a device that:

(A) is primarily designed or produced for the purpose of circumventing a technological measure . . . ;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure . . . ; or

(C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.⁷³

⁶⁶ *Chamberlain*, 292 F. Supp. 2d at 1025.

⁶⁷ *Id.* at 1026.

⁶⁸ *Id.* at 1027.

⁶⁹ *Id.*

⁷⁰ *Id.* at 1028. The Chamberlain GDO software was designed to recognize rolling code values in a “forward window,” which included a large range of values incrementally higher than the last-received rolling code. Previously received signals were included in a “rear window.” To handle the possibility that a user might depress the transmitter many times while outside the range of the GDO receiver, the device was also designed to allow the GDO to operate if a signal outside of both the “forward window” and “rear window” was detected and followed rapidly by a second signal that was greater than the first signal by an increment of three. The Skylink transmitter was designed to mimic this situation and cause the system to resynchronize. *Id.* at 1028-29.

⁷¹ *Id.* at 1032.

⁷² *Chamberlain III*, 381 F.3d 1178, 1185 (Fed. Cir. 2004), *aff’g Chamberlain I*, 292 F. Supp. 2d 1023.

⁷³ 17 U.S.C. § 1201(a)(2) (2000).

Chamberlain charged that the rolling code system was a “technological measure” that “control[led] access” to the copyright-protected rolling code computer program, and that by resynchronizing the GDO system, the defendant’s transmitter “circumvented” Chamberlain’s rolling code system.⁷⁴ Chamberlain further alleged that the defendant’s after-market transmitter (A) was primarily designed or produced for the purpose of circumventing Chamberlain’s rolling code system, (B) had only limited commercially significant purpose or use other than to circumvent, and (C) was marketed for use in circumventing Chamberlain’s technological measure.⁷⁵ Notably, Chamberlain did not allege that the defendant infringed its copyright on the computer program or was liable for contributory copyright infringement.⁷⁶

In defense, Skylink argued that (1) Chamberlain failed to demonstrate that its GDO computer programs were copyrightable, (2) its transmitter served many functions unrelated to circumvention, (3) consumers using the Skylink transmitter to activate the Chamberlain GDO had Chamberlain’s implied consent, (4) Skylink’s activities fell under the interoperability exception of § 1201(f), and (5) Chamberlain’s rolling code program did not protect a copyrighted *work* (i.e., the computer program) but instead protected an uncopyrightable *process* (i.e., the computer program’s function).⁷⁷ Chamberlain responded that it had never given explicit authorization to its consumers to circumvent its rolling code system and that, in any event, Skylink bore the burden of proving that its activities were authorized.⁷⁸

The District Court for the Northern District of Illinois granted the defendant’s motion for summary judgment on the DMCA claim.⁷⁹ The court based its rulings on the issue of authorization and consent, noting that circumvention of a technological measure was defined as an action carried out *without the authority* of the copyright owner (i.e., Chamberlain). The court found that because Chamberlain did not place any conditions on the sale of its GDO, there was an implied authorization, and therefore no circumvention as a matter of law.⁸⁰ The district court warned that holding otherwise would mean that even the homeowners who purchased and used the Skylink transmitter to activate the Chamberlain GDO would be in violation of the DMCA.⁸¹

⁷⁴ *Chamberlain III*, 381 F.3d at 1186.

⁷⁵ *Id.*

⁷⁶ *Id.* at 1185.

⁷⁷ *Id.* at 1186.

⁷⁸ *Id.* at 1186–87.

⁷⁹ *Id.* at 1188.

⁸⁰ *Chamberlain II*, 292 F. Supp. 2d at 1043.

⁸¹ *Id.* at 1039–40.

C. *The DMCA and Toner Printer Cartridges*

In contrast to the decision in *Chamberlain II*, the District Court for the Eastern District of Kentucky found that the defendant's sale of after-market printer toner cartridges could be a violation under the DMCA in *Lexmark I*.⁸² The *Lexmark* plaintiff, a manufacturer of laser printer toner cartridges, brought suit to enjoin the defendant from selling a microchip that enabled the use of replacement printer toner cartridges.⁸³ Lexmark's toner cartridge contained a copyrighted "Toner Loading Program" that measured the amount of toner remaining in the cartridge, and the Lexmark printer contained a copyrighted "Printer Engine Program" that controlled the functions of the printer.⁸⁴ In order for the Lexmark printer to operate, the toner cartridge microchip had to satisfy a "secret handshake" authentication sequence with the Lexmark printer.⁸⁵ The defendant, Static Control, sold a "SMARTEK" microchip that could simulate Lexmark's secret code and enable a third-party toner cartridge to satisfy the Lexmark authentication sequence.⁸⁶

Lexmark alleged that Static Control violated § 1201(a)(2) of the DMCA because Static Control's "SMARTEK" microchip circumvented a "technological measure," the authentication sequence that "controls access" to copyright-protected programs (the Toner Loading Program and Printer Engine Program).⁸⁷ Lexmark argued that Static Control was liable because (A) the microchip was primarily designed or produced for the purpose of circumventing Lexmark's authentication sequence, which effectively controls access to Lexmark's copyrighted programs, (B) Static Control's microchip had only a limited commercially significant purpose or use other than to circumvent the authentication sequence, and (C) Static Control marketed the microchip for use in circumventing Lexmark's authentication sequence.⁸⁸ Unlike in the *Chamberlain* cases, the plaintiff here also alleged infringement of its copyright for both the Toner Loading Program and Printer Engine Program.⁸⁹ Indeed, the parties agreed that the Printer Engine Program was protected by copyright.⁹⁰

The District Court for the Eastern District of Kentucky concluded that the meaning of § 1201(a)(2) of the DMCA was "clear" and accordingly it

⁸² *Lexmark I*, 253 F. Supp. 2d 943, 943 (E.D. Ky. 2003).

⁸³ *Id.* at 947.

⁸⁴ *Id.* at 949, 951.

⁸⁵ *Id.* at 952–53.

⁸⁶ *Id.* at 955.

⁸⁷ *Id.*

⁸⁸ *Id.* at 955–56.

⁸⁹ *Lexmark II*, 387 F.3d 522, 531 (6th Cir. 2004).

⁹⁰ *Id.* at 546.

was “inappropriate” to consider the legislative history.⁹¹ Recognizing that the statute did not define “access,” the court gave it the ordinary, customary meaning, “to enter, to obtain or to make use of.”⁹² The court concluded that because Lexmark’s authentication sequence controlled the consumer’s ability to “make use of” a copyrighted program, the authentication sequence controlled “access.”⁹³ Accordingly, Static Control’s use and trafficking of the “SMARTEK” microchip, which circumvented the authentication sequence, constituted a violation of the DMCA.⁹⁴

The contrasting district court decisions in *Chamberlain II* and *Lexmark I* left many confused and wondering which interpretation of the DMCA would prevail. Many critics felt that the district court in *Lexmark* had improperly applied the DMCA to extend Lexmark’s after-market monopoly rather than to combat true digital piracy, as Congress had envisioned.⁹⁵ When the *Chamberlain II* and *Lexmark I* cases both went up on appeal, critics anxiously waited to see if the broad construction of the DMCA applied by the district court in *Lexmark* would be accepted by either the Federal Circuit or the Sixth Circuit. When the Federal Circuit rejected a broad construction of the DMCA’s antitrafficking provision, which would have encompassed durable goods in its scope, in favor of a requirement that there be a “reasonable relation” between circumvention and copyright infringement, the critics breathed a sigh of relief.

III. ANALYSIS OF THE DMCA

The Federal Circuit and Sixth Circuit faced the same issue on appeal—how should the antitrafficking provision of the DMCA be construed? The Federal Circuit, the first court to render its opinion, flatly rejected a broad construction of the DMCA’s antitrafficking provision, which would have encompassed durable goods. Less than two months later, the Sixth Circuit ruled in *Lexmark*, also rejecting a broad construction of the antitrafficking provision. In reaching their conclusions, both the Federal Circuit and Sixth Circuit relied on the legislative history of the DMCA as a guide.⁹⁶ Nonetheless, the two appeals courts decided on two markedly different interpretations of the antitrafficking provision: the Federal Circuit narrowly interpreted “access” to require a connection to copyright infringement and

⁹¹ *Lexmark I*, 253 F. Supp. 2d at 967 (“The plain meaning of the DMCA is clear and it would be inappropriate for the Court to consider the legislative history in an effort to determine the “true” congressional intent.”).

⁹² *Id.*

⁹³ *Id.* at 967–68.

⁹⁴ *Id.*

⁹⁵ See, e.g., Elec. Frontier Found., *supra* note 5.

⁹⁶ *Chamberlain III*, 381 F.3d 1178, 1196 (Fed. Cir. 2004); *Lexmark II*, 387 F.3d 522, 549 (6th Cir. 2004).

the Sixth Circuit narrowly interpreted “effectively” to require that access to the copyright-protected work be unavailable except through circumvention.

A. The Federal Circuit’s Ruling in Chamberlain Group v. Skylink Technologies

The Court of Appeals for the Federal Circuit affirmed the Northern District of Illinois’s finding of no liability under the DMCA.⁹⁷ After clarifying the complex jurisdictional basis for hearing the appeal,⁹⁸ the court proceeded to discuss Chamberlain’s claim under the DMCA.⁹⁹ The court began its analysis by rejecting Chamberlain’s contention that the DMCA established a new property right akin to that created by the grant of a copyright or patent.¹⁰⁰ Chamberlain argued that the DMCA “empowered manufacturers” to make it per se illegal for consumers to use embedded software products in conjunction with competing after-market products absent express authorization.¹⁰¹ The court warned that if the DMCA established such a property right, the statute would in effect exempt manufacturers like Chamberlain from both antitrust laws and the doctrine of copyright misuse.¹⁰² The court stated that the DMCA merely expanded liability by establishing new causes of action under which copyright owners could secure their property (i.e., the copyrighted work).¹⁰³

The court further explained that the DMCA envisioned a property-liability distinction, evidenced by the fact that it defined circumvention as an activity undertaken *without authority*.¹⁰⁴ Accordingly, in contrast to copyright law, where the defendant has the burden of asserting authorization as an affirmative defense to infringement,¹⁰⁵ under the DMCA it is the plaintiff who bears the significant burden of proving that the defendant’s access was *unauthorized*.¹⁰⁶

⁹⁷ *Chamberlain III*, 381 F.3d at 1178.

⁹⁸ *Id.* at 1188–92. The court asserted that it had jurisdiction to hear the appeal under 28 U.S.C. § 1295(a)(1) (2000) because the district court’s jurisdiction arose under the patent laws. *Id.* at 1188–90. This assertion of jurisdiction is questionable since Chamberlain’s patent claim was dismissed by the trial court without prejudice but subject to a condition subsequent (the outcome of another pending court case). By the time of the appeal, the condition subsequent had ripened into a dismissal with prejudice such that the patent claim had, in effect, been adjudicated on its merits and Chamberlain could no longer reassert the patent claim in any forum. Since the patent claim could no longer be appealed, it seems that the Federal Circuit could not have had jurisdiction under 28 U.S.C. § 1295(a)(1).

⁹⁹ *Chamberlain III*, 381 F.3d at 1192.

¹⁰⁰ *Id.* at 1192–93 (“[T]he DMCA’s text indicates that circumvention is not infringement.”).

¹⁰¹ *Id.* at 1193.

¹⁰² *Id.*

¹⁰³ *Id.* at 1193–94.

¹⁰⁴ *Id.* at 1193.

¹⁰⁵ *See, e.g., Feist Publ’ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361 (1991).

¹⁰⁶ *Chamberlain III*, 381 F.3d at 1193.

The Federal Circuit next rejected Chamberlain's proposed construction of the DMCA. Chamberlain's interpretation severed the connection between the access control measure and infringement of the copyright-protected work.¹⁰⁷ The court declared that both the statutory structure and legislative history of the DMCA made it "clear" that the anticircumvention and antitrafficking provisions of § 1201 applied only to circumventions that were "reasonably related to protected rights."¹⁰⁸ Thus, defendants would only be liable under the provisions of § 1201 if they used or trafficked a device that circumvented access controls "in ways that facilitate infringement."¹⁰⁹

Relying upon the statutory language, the court noted that "virtually every clause of § 1201 that mentions 'access' links 'access' to 'protection.'"¹¹⁰ The court concluded that the overall structure of the DMCA provisions supported the existence of a relationship between circumvention and the protected right.¹¹¹ Specifically, the court pointed out that § 1201(b) prohibits trafficking in devices that circumvent the protection afforded by a technological measure, and that persons who directly circumvent the protection of the technological measure would be liable for copyright infringement, an act already prohibited by the Copyright Act.¹¹²

The court also found support for its conclusion in the DMCA's legislative history—in particular, a Senate report which seemed to acknowledge the link between access and protection. Specifically, the Senate report asserted that defendants who trafficked in devices that circumvented rights-control measures (as opposed to access-control measures) that protected copyrighted works necessarily facilitated copyright infringement. Congress enacted § 1201(b) only to further enforce the existing prohibition on copyright infringement.¹¹³ Also because the direct act of circumvention of an access control measure was not previously prohibited, Congress enacted § 1201(a)(1) to make circumvention unlawful, and enacted the corresponding device antitrafficking limitation in § 1201(a)(2) to further bolster the an-

¹⁰⁷ *Id.* at 1197.

¹⁰⁸ *Id.* at 1195. It should be noted that the "reasonably related" language is entirely nonstatutory. For a discussion of the dissonance between the Federal Circuit's construction of the DMCA and the statutory language, see Zohar Efroni, *A Momentary Lapse of Reason: Digital Copyright, The DMCA and a Dose of Common Sense*, 28 COLUM. J.L. & ARTS 249, 285–95 (2005).

¹⁰⁹ *Chamberlain III*, 381 F.3d at 1195. The meaning of "facilitate infringement" was not addressed by the court and so it is an open question whether a device must circumvent an access control measure in a way that *actually* facilitates infringement, *probably* facilitates infringement, *quite possibly* facilitates infringement, or just *is capable of* facilitating infringement.

¹¹⁰ *Id.* at 1197.

¹¹¹ *Id.* at 1195, 1197.

¹¹² *Id.* at 1195.

¹¹³ *Id.* (citing S. REP. No. 105-90, at 12 (1998)).

ticircumvention provision, § 1201(a)(1).¹¹⁴

The court further argued that the text of the DMCA should be interpreted in the context of Congress's theme of balancing the interests of the copyright owners with those of the content users.¹¹⁵ In considering this balance, the court noted that there was a significant difference between defendants whose products enable illegal copying and those whose products enable only legitimate uses of copyrighted software.¹¹⁶ The court stated that the very fact that the DMCA might prohibit noninfringing public uses reflected Congress's decision to rebalance the interests involved by creating different types of liability. The court reasoned that Congress intended to create two distinct types of liability: liability for trafficking in devices that serve as "a 'key' that essentially enables a trespass" upon a copyright, and liability for *actually* infringing the copyright.¹¹⁷

The *Chamberlain III* court acknowledged that the plaintiff's construction that separated circumvention of the access control measure from copyright infringement was plausible—when taken out of context. However, the court found that the plaintiff's interpretation introduced "irreconcilable problems in statutory construction"¹¹⁸ and required a broad reading of the DMCA, something Congress had not intended.¹¹⁹

The court also warned that allowing copyright owners under § 1201(a) to use technological measures to block *all* access to their copyrighted works would effectively create two distinct copyright regimes. The first regime would be one in which copyright owners would possess only the copyrights enumerated in 17 U.S.C. § 106¹²⁰ and the corresponding ability to hold traffickers in circumvention devices liable under § 1201(b) if they chose to incorporate technological measures to protect those enumerated rights from risk of technological encroachment.¹²¹ The second regime would be one in which owners of a work protected by both copyright *and* an access control measure would possess unlimited rights to hold circumventors liable under § 1201(a) merely for accessing the work, even if that access enabled only rights granted by the Copyright Act.¹²² The court asserted that the latter regime would irrationally imply that Congress, in exercising its authority to

¹¹⁴ *Id.* The court noted that trafficking liability under § 1201(a)(2) could not exist in the absence of a violation of § 1201(a)(1). *Id.* at 1196 n.13. For an argument that the Federal Circuit's construction of the DMCA provision is inconsistent with the legislative history, see Efroni, *supra* note 108, at 289–92.

¹¹⁵ *Chamberlain III*, 381 F.3d at 1196.

¹¹⁶ *Id.* at 1198.

¹¹⁷ *Id.*

¹¹⁸ *Id.* at 1199.

¹¹⁹ *Id.* at 1197.

¹²⁰ *Id.* at 1199–1200 (consisting of the exclusive rights to reproduce the work, prepare derivative works, distribute copies, etc., and 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).

¹²¹ *Id.* at 1199.

¹²² *Id.* at 1200.

define the scope of the limited copyright monopoly,¹²³ allowed copyright owners to deny all public access to their copyrighted works.¹²⁴ In addition, the second regime conflicted with § 1201(c)(1) of the DMCA, which prescribes that “[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.”¹²⁵

The court further declared that the broad policy implications of considering “access” in a vacuum devoid of “protection” were both “absurd and disastrous.”¹²⁶ For example, such a 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.”¹²⁷ To allow this would be tantamount to exempting manufacturers from copyright misuse and antitrust laws, something the court derided as flatly “wrong.”¹²⁸

Finally, the court rejected Chamberlain’s contention that its customers were not expressly authorized to circumvent its rolling code. The court stated that entitling a manufacturer to prohibit legitimate purchasers of its product from circumventing a control measure to access copyright protected software contained in the product would allow the manufacturer “to prohibit *exclusively fair* uses even in the absence of any feared foul use.”¹²⁹ The court declared that consumers who purchase a product containing copyrighted software have an “inherent legal right” to use their copy of the software.¹³⁰ Significantly, the court declined to address whether a consumer who circumvented an access control measure to engage in a use permitted by the Copyright Act, but prohibited by contract, would be subject to liability under the DMCA.¹³¹

¹²³ Eldred v. Ashcroft, 537 U.S. 186, 204–05 (2003).

¹²⁴ *Chamberlain III*, 381 F.3d at 1200. For an analysis of whether a copyright owner has the exclusive right to control access to his work, see Efroni, *supra* note 108, at 270–79.

¹²⁵ *Chamberlain III*, 381 F.3d at 1200.

¹²⁶ *Id.* at 1201.

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ *Id.* at 1202. Note that the court’s expression “fair uses” should be understood to include all legal uses including, but not limited to, fair use under 17 U.S.C. § 107 (2000).

¹³⁰ *Chamberlain III*, 381 F.3d at 1202. A purchaser’s right to use their copy of software was recently affirmed by the Second Circuit in *Krause v. Titleserv, Inc.*, 402 F.3d 119 (2d Cir. 2005).

¹³¹ *Chamberlain III*, 381 F.3d at 1202 n.17. This question is of particular interest in view of the Federal Circuit’s decision, in *Bowers v. Baystate Techs., Inc.*, that a shrinkwrap contract provision was enforceable and not preempted by copyright law. 320 F.3d 1317 (Fed. Cir. 2003). If such a contract provision were enforceable, circumvention of the access control measure in order to make even fair use of a copyright work would presumably be a DMCA violation—because it was without authorization—meaning that a durable goods manufacturer such as Chamberlain could use the DMCA in combination with contract law in order to create an after-market monopoly.

The court concluded by announcing a test for establishing liability under § 1201(a)(2) of the DMCA.¹³² To establish a prima facie case, a plaintiff must prove six elements: (1) ownership of a valid copyright on a work that is (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.¹³³

For the purposes of appeal, the court assumed that Chamberlain owned a valid copyright in its computer program.¹³⁴ The court further assumed that the computer program, which verified the rolling code, was a technological measure that effectively controlled access.¹³⁵ Applying its new standard, the court concluded that Chamberlain had failed to satisfy elements (4) and (5) of the test: Element (4) was not satisfied because Chamberlain could not establish that Skylink lacked authorization. Element (5) was not satisfied because Chamberlain could not explain how the access gained facilitated infringement of the copyright on the computer program in view of the fact that Skylink's transmitter did not make use of Chamberlain's copyrighted computer program, but rather sidestepped it altogether.¹³⁶

B. *The Sixth Circuit's Ruling in Lexmark v. Static Control Components*

Soon after the Federal Circuit's decision in *Chamberlain III*, the Sixth Circuit issued its opinion in *Lexmark II*.¹³⁷ The court disagreed with the district court's conclusion that the meaning of § 1201(a)(2) of the DMCA was "clear." The court stated that it was instead the consumer's purchase of the Lexmark printer, rather than the circumvention of the authentication sequence, that allowed them "access" to the program.¹³⁸ To reach this conclusion, the court observed that since the Printer Engine Program and Toner Loading Program were not encrypted, the purchaser could decompile the program without using or bypassing the authentication sequence.¹³⁹ Thus, the authentication sequence blocked one form of access to the protected

¹³² *Chamberlain III*, 381 F.3d at 1203.

¹³³ *Id.*

¹³⁴ *Id.* at 1185 n.4.

¹³⁵ *Id.* at 1204. It is notable that the Federal Circuit in *Chamberlain III* assumed the existence of effective access control while, on the other hand, it was the absence of effective access control that was the critical factor that led to the Sixth Circuit's holding in *Lexmark II*.

¹³⁶ *Id.*

¹³⁷ *Lexmark II*, 387 F.3d 522, 546 (6th Cir. 2004).

¹³⁸ *Id.*

¹³⁹ *Id.*

program while leaving other forms of access open.¹⁴⁰ The court held that because the authentication sequence did not control all means of access, the authentication sequence did not “effectively” control access to the protected program as required by the DMCA.¹⁴¹

The court explained that the DMCA only applies where 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,” where the manufacturer guards against all access to the copyrighted work by using the technological measure.¹⁴² The court contrasted this vision with the copyrightable expression in *Lexmark*, which operated “only on one plane: in the literal elements of the program,” and whose output was “purely functional” (i.e., to make a printer operate).¹⁴³ The court noted that “[n]owhere 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.”¹⁴⁴

Accordingly, because *Lexmark* had not directed any security efforts, through the authentication sequence or otherwise, to ensure that its copyrighted work could not be read and copied, the court concluded that *Lexmark*’s claim under the DMCA must fail.¹⁴⁵

Judge Merritt concurred in the judgment, but stressed that the key question was the “purpose” of the circumvention technology.¹⁴⁶ The judge suggested that the statute should be read to “[require] plaintiffs as part of their burden of pleading and persuasion to show a purpose to pirate on the part of defendants.”¹⁴⁷ Here the defendant’s purpose was, like that in *Chamberlain*, to simply sidestep the plaintiff’s copyrighted material, not to pirate it. District Judge Feikens, who concurred in the judgment with respect to the DMCA claim, echoed this by stating that “there is an element of scienter present in the DMCA.”¹⁴⁸

¹⁴⁰ *Id.* at 547.

¹⁴¹ *Id.*

¹⁴² *Id.* at 548.

¹⁴³ *Id.* at 549.

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

¹⁴⁶ *Id.* at 552 (Merritt, J., concurring).

¹⁴⁷ *Id.*

¹⁴⁸ *Id.* at 562 (Feikens, D.J., concurring in part and dissenting in part). Judge Feikens’s concurrence on the DMCA claim was narrowly based on the fact that the plaintiff had failed to prove that the defendant knew the Toner Loading Program was on the toner cartridge. Judge Feikens reasoned that, although consumers gained access to the Printer Engine Program by purchasing the printer, the consumers did not gain access to the Toner Loading Program via an implied license contained on the Prebate toner cartridge because they purchased it subject to a shrink wrap agreement. *Id.* at 563.

C. *Analyzing the DMCA in View of Chamberlain and Lexmark*

The starting point for interpreting the meaning of the DMCA, in view of the decisions in *Chamberlain III* and *Lexmark II*, is the language of the statute itself.¹⁴⁹ The provision at issue in both the *Chamberlain* and *Lexmark* cases is § 1201(a)(2), which states:

No person shall manufacture, import, 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 this title;

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

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.¹⁵⁰

The Act defines "circumvent a technological measure" as "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."¹⁵¹ The Act further states that a technological measure "effectively controls access to a work" if it "requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."¹⁵²

The district court's finding in *Lexmark* that the broad language of § 1201(a)(2) was "clear" such that resort to legislative history was inappropriate¹⁵³ was surprising considering the multitude of DMCA critics who consider the anticircumvention provisions ambiguous.¹⁵⁴ Despite the lower

¹⁴⁹ See *Good Samaritan Hosp. v. Shalala*, 508 U.S. 402, 409 (1993) ("The starting point in interpreting a statute is its language, for '[i]f the intent of Congress is clear, that is the end of the matter.'" (quoting *Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 842 (1984))).

¹⁵⁰ 17 U.S.C. § 1201(a)(2) (2000).

¹⁵¹ *Id.* § 1201(a)(3)(A).

¹⁵² *Id.* § 1201(a)(3)(B).

¹⁵³ *Lexmark I*, 253 F. Supp. 2d 943, 967 (E.D. Ky. 2003). Statutory language that is unambiguous is generally regarded as conclusive except when literal application of a statute will produce a result demonstrably at odds with the intentions of its drafters or when the statutory language is ambiguous. See *Reves v. Ernst & Young*, 507 U.S. 170, 177 (1993); *Nixon v. Kent County*, 76 F.3d 1381, 1386 (6th Cir. 1996) (citing *Kelley v. E.I. DuPont de Nemours & Co.*, 17 F.3d 836, 842 (6th Cir. 1994)).

¹⁵⁴ See, e.g., David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909, 964 (2002) (calling the language of the DMCA impenetrable); David Nimmer, *Puzzles of the Digital Millennium Copyright Act*, 46 J. COPYRIGHT SOC'Y

court's determination that the statutory language was unambiguous, neither the Sixth Circuit nor the Federal Circuit refrained from looking to the legislative history in rejecting a broad construction of the DMCA provision.¹⁵⁵ In *Chamberlain II*, the Federal Circuit concluded that the plain meaning of the DMCA was "absurd" and at odds with clear legislative intent. In contrast, the *Lexmark II* court concluded that the statutory language was ambiguous. Is the text of the DMCA really ambiguous? If the text is not ambiguous, does a literal interpretation of § 1201(a)(2) produce a result that is demonstrably at odds with the intent of the drafters?

I. Access.—The first source of possible ambiguity is the use of the term "access." Recall that § 1201(a)(2) creates liability for "circumventing a technological measure that effectively controls access to a work protected under this title," where "this title" refers to the Copyright Act.¹⁵⁶ Although the DMCA defines when a technological measure "effectively controls access to a work,"¹⁵⁷ the term "access" is not further defined by the statute. The literal text of § 1201(a)(2) does not state that "access" is connected to the "right of the copyright owner under this title."¹⁵⁸ The lack of an implicit textual connection suggests that liability may depend solely on circumvention of a technological measure that controls "access," without regard to whether circumvention is in any way related to copyright infringement.¹⁵⁹ The district court in *Lexmark I* defined "access" according to its "ordinary, customary meaning," which is "the ability to enter, to obtain, or to make use of."¹⁶⁰ On appeal, the Sixth Circuit in *Lexmark II* also relied on this ordinary meaning.¹⁶¹

Applying this broad definition of "access" to the plain text of the statute results in a construction of the DMCA that extends liability to circumvention of technological measures that restrict access for noninfringing activities as well as for infringing activities.¹⁶² For example, if an individual purchases a game that requires entry of a password from the purchaser's

U.S.A. 401, 441 n.216 (1999) (same); Samuelson, *supra* note 5, at 524 (calling the DMCA provisions "highly ambiguous").

¹⁵⁵ The appellate court decisions in *Chamberlain III* and *Lexmark II* reflect the courts' desire to inject flexibility into the otherwise rigid statutory text. See Stacy L. Dogan & Joseph P. Liu, *Copyright Law and Subject Matter Specificity: The Case of Computer Software*, 61 N.Y.U. ANN. SURV. AM. L. 203, 232–33 (2005).

¹⁵⁶ 17 U.S.C. § 1201(a)(2).

¹⁵⁷ *Id.* § 1201(a)(3)(B) ("[A] technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.").

¹⁵⁸ *Id.* § 1201(a)(2).

¹⁵⁹ See Ginsburg, *supra* note 5, at 140–41.

¹⁶⁰ *Lexmark I*, 253 F. Supp. 2d 943, 967 (E.D. Ky. 2003) (citing MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 6 (10th ed. 1999)).

¹⁶¹ *Lexmark II*, 387 F.3d 522, 546 (6th Cir. 2004).

¹⁶² Ginsburg, *supra* note 5, at 140–41.

computer in order to access the copyright-protected game, the access control measure (the password requirement) would prevent the purchaser from unlawfully copying and distributing the game to the public (an infringing use). However, the password requirement would also prevent the purchaser from lawfully playing the game on a friend's computer (a noninfringing use under the "first-sale doctrine").¹⁶³ Thus, under this definition of access, trafficking a circumvention device designed and marketed for a noninfringing use will still be barred under § 1201(a)(2) unless the noninfringing use of that device is of more than "limited commercial significance."¹⁶⁴

However, "access" as used in copyright law customarily means an "opportunity . . . to see, hear, or copy a copyrighted work."¹⁶⁵ Thus, in the context of copyright law, "access" arguably has a narrower scope: one relating to the ability to perceive the copyrighted work.¹⁶⁶ Perception of a work is different for tangible copyrighted materials, such as a story in a book which one can read directly from the printed page, and digital works where one must use a machine to convert imperceptible text (e.g., object code) into perceptible sound or images.¹⁶⁷ This distinction is important because unlike traditional, tangible works, digital works can be *obtained* without actually *perceiving* them.¹⁶⁸

Thus, how access is defined can have a profound impact on liability under the DMCA. Under a broad definition of access, such as that adopted

¹⁶³ *Id.*

¹⁶⁴ Section 1201(a)(2) specifies three disjunctive conditions for liability: that the device

(A) is primarily designed or produced for the purpose of circumventing a technological measure . . . ; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure . . . ; or (C) is marketed . . . for use in circumventing a technological measure.

17 U.S.C. § 1201(a)(2) (2000) (emphasis added); *see also* Reese, *supra* note 39, at 630.

¹⁶⁵ BLACK'S LAW DICTIONARY 14 (8th ed. 2004); *see also* General Universal Sys. v. Lee, 379 F.3d 131, 141 (5th Cir. 2004) ("[An] access element is satisfied if the person who created the allegedly infringing work had a reasonable opportunity to view the copyrighted work."); Ellis v. Diffie, 177 F.3d 503, 506 (6th Cir. 1999) ("Access is essentially 'hearing or having a reasonable opportunity to [view] the plaintiff[s] work and thus having the opportunity to copy.'" (quoting Tree Publ'g Co. v. Warner Bros. Records, 785 F. Supp. 1272, 1274 (M.D. Tenn. 1991))); BLACK'S LAW DICTIONARY 13 (7th ed. 1999) (defining "access" as the "opportunity to view or copy a copyrighted work").

¹⁶⁶ *See* 2 PAUL GOLDSTEIN, COPYRIGHT § 9.2.1.1, at 9:9 (3d ed. 2005) (stating that "access" can be described as reading, seeing, or hearing a work); 2 PAUL GOLDSTEIN, COPYRIGHT § 5.17.1, at 5:245 (2d ed. 1996 & 2000 Supp.) (stating that access to a work occurs any time a user derives value from the work); Jane C. Ginsburg, *From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law*, 50 J. COPYRIGHT SOC'Y U.S.A. 113, 115 (2003), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222493 (stating that access is required in every act of perception or materialization of a digital copy); Reese, *supra* note 39, at 633 ("Access to a work stored in digital format requires the ability to perceive that work: to see the text, hear the recorded sound, and view the visual images."); *see also* Hurwitz, *supra* note 5, at 269 (proposing to define access as used in § 1201 as "the ability to perceive a writing, audiovisual work, performance or phonogram, or to manually execute a computer software application").

¹⁶⁷ Reese, *supra* note 39, at 633.

¹⁶⁸ For a discussion of digital access, *see* Efroni, *supra* note 108, at 298–300.

by the district court in *Lexmark I*, there could be liability under the DMCA for circumventing a technological measure even if the measure in no way controlled “access” to a means of perceiving a copyrighted work. For example, a car owner could be liable under the DMCA for circumventing a copyrighted authentication sequence employed by Ford Motor Company in order to gain access to the proper functioning or use of an after-market replacement oil filter sold by a competitor. Under the narrower interpretation suggested by traditional copyright law, the act of circumventing a technological control would not be a violation of the DMCA, unless one subsequently was *capable of perceiving* a copyrighted work as a result of the circumvention. Thus under a narrow definition of access, circumventing a content scrambling system (“CSS”) which prevents one from perceiving a movie on a DVD would still be a DMCA violation consistent with Congress’s intent. On the other hand, circumventing an authentication sequence on a toner cartridge without perceiving, or being capable of perceiving, any copyrighted software would not be a violation of the DMCA.

Unlike the district court and Sixth Circuit in the *Lexmark* decisions, the Federal Circuit in *Chamberlain III* did not directly address the meaning of the term “access.”¹⁶⁹ Instead, the Federal Circuit concluded that the structure of the DMCA and the legislative intent “both make it clear” that access be “reasonably related” to protection under the Copyright Act.¹⁷⁰ Requiring access to be “reasonably related” to protection of a copyrighted work has the same substantive effect as narrowly defining “access” as an opportunity to perceive a copyrighted work; both approaches tie access back to copyright protection.

For example, circumventing a CSS that prevents one from accessing a movie on a DVD would be a violation under the *Chamberlain* definition because the access control is *reasonably related* to protection of the copyrighted movie (that is, the access would facilitate copying of the movie and thus copyright infringement). In contrast, circumventing an authentication sequence on a toner cartridge would not be a violation of the DMCA under *Chamberlain* because although the circumvention allows access in the broader sense, the access is not related to a copyright violation (the access gained enables one to use the toner cartridge but does not enable one to copy the copyrighted code).¹⁷¹

2. *Effectively*.—Section 1201(a)(2) prohibits trafficking in a device that circumvents a technological measure that effectively controls access to

¹⁶⁹ *Chamberlain III*, 381 F.3d 1178, 1195 (Fed. Cir. 2004).

¹⁷⁰ *Id.*

¹⁷¹ Both acts of circumvention would be a violation under the broader definition of access relied on in *Lexmark* because the circumvention provides “access” to or “the ability to make use of” a copyright protected work. There is no requirement that the access leads to the ability to make use of the work in a way that is at all related to copyright infringement.

a copyright-protected work. This provision contains another source of textual ambiguity: the term “effectively.”¹⁷² This term is not defined in the statute,¹⁷³ and is ambiguous because one may assign it two distinct meanings: “in an effective way,” or simply “in effect.”¹⁷⁴ Thus, in the context of the DMCA, a broad definition of “effectively” would mean that the technological measure must “in effect” control access to the copyrighted work (i.e., in at least some nominal way). Alternatively, a narrow definition of “effectively” would mean that the technological measure must successfully control access to the work (i.e., must control *all* access to the work).

The meaning of the term “effectively” was addressed by the Southern District of New York in *Universal City Studios, Inc. v. Reimerdes*.¹⁷⁵ There, the court rejected the defendant’s argument that the DMCA only applied to technological measures that were a “strong means” of protecting copyrighted works.¹⁷⁶ Instead, the court concluded that a technological measure effectively controlled access to a copyrighted work if its *function* was to control access, thereby adopting a broad definition of “effectively.”¹⁷⁷ The court remarked that the plaintiff’s encryption code “actually work[ed]” to prevent access to the protected work and thus effectively controlled access to the work.¹⁷⁸ The court in *Universal Studios* noted that to define “effectively” to mean “successfully” or “efficaciously” would “gut the statute” because all circumvented technological measures would be ineffective by definition.¹⁷⁹

In *Lexmark II*, the Sixth Circuit also considered the meaning of the term “effectively.”¹⁸⁰ The *Lexmark II* court concluded that although the plaintiff’s authentication sequence blocked one form of access, the copyrighted program could also be accessed directly by decompiling the object code.¹⁸¹ The court explained that § 1201(a)(3) states that the technological

¹⁷² 17 U.S.C. § 1201(a)(2) (2000).

¹⁷³ The DMCA merely defines when a technological measure “effectively controls access to a work.” *Id.* § 1201(a)(3)(B).

¹⁷⁴ *See, e.g.*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 570 (4th ed. 2000).

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

¹⁷⁶ *Id.* at 317–18. The defendant argued that the encryption software, based on a 40-bit encryption key, was a “weak cipher” and not protected by the DMCA. *Id.*

¹⁷⁷ *Id.* (citing HOUSE COMM. ON JUDICIARY, SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, at 10 (Comm. Print 1998)).

¹⁷⁸ *Id.* at 318. The court also noted that the House Commerce Committee made it clear that measures based on encryption or scrambling “effectively control” access to copyrighted works. *Id.*

¹⁷⁹ *Id.*

¹⁸⁰ *Lexmark II*, 387 F.3d 522, 547 (6th Cir. 2004). The Sixth Circuit in *Lexmark II* cited the decision in *Universal City Studios, Inc. v. Reimerdes* but distinguished the case factually because it did not involve a situation where the access control measure left the literal code of the program freely readable. *Id.* at 547.

¹⁸¹ *Id.* at 548.

measure must “require[] the application of information, or a process or a treatment . . . to gain access to the work.”¹⁸² Accordingly, the court concluded that the authentication sequence could not “effectively” control access to a protected work if another means of access remained open, thus adopting a narrow interpretation of “effectively.”¹⁸³

Though the interpretations of “effectively” provided by the courts in *Lexmark II* and *Universal Studios* appear contradictory, they can be reconciled. Specifically, the interpretations could be taken to mean that a technological measure will “effectively control access” so long as it controls all avenues of access to the work, even if the means of technological control is not very successful. However, this combined interpretation does not resolve all the ambiguity surrounding “effectively.” For example, it remains unclear whether a court would consider an encryption measure to “effectively” control access if the code that would break the encryption were readily available such that only a very small number of people would actually be prevented from accessing the work. Moreover, the court’s position in *Lexmark II*¹⁸⁴ could suggest that, had Lexmark simply used a rights control measure (such as encryption) to prevent users from accessing the Printer Engine Program, the authentication sequence might have been considered to have “effectively” controlled access to that program such that there would have been a violation of § 1201(a)(2) of the DMCA.

3. *Intent.*—Section 1201(a)(2) sets forth three alternative elements for a finding of liability, which relate to the alleged trafficker’s purpose or intent in producing and marketing a circumvention device.¹⁸⁵ Specifically the statute looks at why the device was designed or produced, what commercial purpose the device has other than for circumvention, and how the device is marketed.¹⁸⁶

The presence of an intent requirement did not go unnoticed by the appellate courts. In affirming the district court’s ruling, the Federal Circuit in *Chamberlain III* commented that the court had analyzed the allegations “in precisely the appropriate manner—a narrow focus on Skylink’s behavior, *intent*, and product.”¹⁸⁷ Similarly in *Lexmark II*, two judges on the three-judge panel, Judge Merritt and Judge Feikens, who both concurred in the Sixth Circuit’s judgment of the DMCA claim, commented on the intent of the defendant. Judge Merritt stated that the key question was the “pur-

¹⁸² *Id.* at 547 (alteration in original).

¹⁸³ *Id.* at 549.

¹⁸⁴ *Id.* (“Because Lexmark has not directed any of its security efforts, through its authentication sequence or otherwise, to ensuring that its copyrighted work . . . cannot be read and copied, it cannot lay claim . . . under [the DMCA].”).

¹⁸⁵ 17 U.S.C. § 1201(a)(2) (2000).

¹⁸⁶ *Id.*

¹⁸⁷ *Chamberlain III*, 381 F.3d 1178, 1203 (Fed. Cir. 2004) (emphasis added).

pose” of the circumvention technology¹⁸⁸ and suggested that plaintiffs should demonstrate that the defendants had “a purpose to pirate.”¹⁸⁹ Judge Feikens noted that there was “an element of scienter” in the DMCA.¹⁹⁰

Despite their recognition of this issue, both the *Chamberlain III* and *Lexmark II* courts reached their conclusions based upon access (either its relation to copyright infringement or its being completely controlled by the technological measure) and therefore did not articulate a standard regarding the level of intent required.¹⁹¹ Notably, the test set forth in *Chamberlain III* failed to include any element of intent.¹⁹² Nevertheless, intent played some role in the courts’ analyses, which suggests that the defendant’s intent may prove to be an important element of a DMCA analysis in future decisions.

4. *Ownership of a Valid Copyright.*—One final source of ambiguity in the DMCA provisions is whether a plaintiff who asserts a DMCA claim must itself own a copyright or whether the plaintiff must merely demonstrate that someone owns a valid copyright. In the *Chamberlain* and *Lexmark* cases, the plaintiffs owned the copyrights to the computer programs to the extent those programs were copyrightable. However, the *Chamberlain* test established that the plaintiff must demonstrate “ownership of a valid copyright.”

According to § 1203(a) of the DMCA, “any person” can file suit for a violation of either § 1201 or § 1202.¹⁹³ At least one court has concluded that the plaintiff need not be the copyright owner. In *Comcast of Illinois X, L.L.C. v. Hightech Electronics, Inc.*,¹⁹⁴ Comcast filed a claim under § 1201(a)(2) of the DMCA for circumventing a descrambling method (i.e., a technological measure) protecting certain copyrighted programs. However, Comcast was not the copyright holder of the programs on the networks that it provided to its subscribers. Rather Comcast merely controlled access to such protected material by controlling the technological measure that protected the copyrighted material. The Northern District of Illinois held that civil remedies were not limited to the copyright holder and that, so long as Comcast was the injured party, it could bring suit pursuant to the DMCA.¹⁹⁵

¹⁸⁸ *Lexmark II*, 387 F.3d at 552 (Merritt, J., concurring).

¹⁸⁹ *Id.*

¹⁹⁰ *Id.* at 562 (Feikens, J., concurring in part and dissenting in part).

¹⁹¹ *See supra* Part III.A–B.

¹⁹² *See supra* notes 132–133 and accompanying text.

¹⁹³ 17 U.S.C. § 1203(a) (2000).

¹⁹⁴ No. 03 C 3231, 2004 U.S. Dist. LEXIS 14619 (N.D. Ill. July 28, 2004).

¹⁹⁵ *Id.* at *17–18 (“[P]ursuant to 17 U.S.C. § 1203(a) ‘any person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation.’”).

D. Conclusion Regarding Courts' Interpretations

The foregoing analysis of the DMCA in view of the appellate courts' decisions in *Chamberlain III* and *Lexmark II* illustrates the problems with interpreting § 1201(a)(2) and the many ambiguities that lie within the statute. The *Chamberlain* court was the first appellate court to face head-on the tension between the rights of copyright owners, and the traditional rights of users brought on by the DMCA in the context of durable goods. In so doing, the court disposed of a broad, literal interpretation of the statute, calling it "absurd." The court in *Chamberlain III* did not find ambiguity per se; rather, it boldly concluded that the plain meaning of the DMCA, if literally applied, would produce a result that was clearly at odds with the intent of Congress in enacting the DMCA and would raise significant antitrust issues.¹⁹⁶ In contrast, the Sixth Circuit in *Lexmark II* justified its reliance on legislative history by finding ambiguity in the language of the statute instead of concluding that the plain meaning of the statute was "absurd."

In view of the foregoing, it seems clear that a broad interpretation of the statutory text, which would extend DMCA liability to the durable goods realm, leads to a result in direct conflict with the statute's purpose to protect copyrighted digital content in the stream of electronic commerce.¹⁹⁷ Accordingly, the courts were justified in relying on the legislative intent to aid in statutory interpretation, thereby avoiding a conflicting result. Now that the Federal Circuit and Sixth Circuit have tried their hand at interpreting the DMCA, the question is whether we can live with the DMCA as it is now construed.

IV. EVALUATION OF THE *CHAMBERLAIN* TEST

In *Chamberlain III*, the court set forth six elements a plaintiff must prove in order to establish a prima facie case under § 1201(a)(2) of the DMCA:

(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.¹⁹⁸

Thus, according to the court, the copyright owner must prove in element (5) the existence of a "reasonable relationship between the circumvention at issue and a use relating to a property right for which the Copyright Act per-

¹⁹⁶ See *supra* notes 126–128 and accompanying text.

¹⁹⁷ See H.R. REP. No. 105-551, pt. 2, at 26 (1998).

¹⁹⁸ *Chamberlain III*, 381 F.3d 1178, 1203 (Fed. Cir. 2004).

mits the copyright owner to withhold authorization—as well as notice that authorization was withheld.”¹⁹⁹

Applying the *Chamberlain* test to a series of fact patterns should demonstrate whether this test is workable, and whether this test produces results consistent with the congressional intent behind the DMCA. If the test is “workable,” it should consistently find liability under § 1201(a)(2) for classic circumvention actions to which the DMCA was specifically targeted—for example, cases involving digital piracy. Conversely, the test should not find liability for circumvention actions in cases that do not involve digital content products.

Initially the *Chamberlain* test is applied to the facts of the *Lexmark* cases discussed above to determine if the test results are consistent with the Sixth Circuit’s finding of no liability. Then, the test is applied to two cases related to piracy involving computer video game services and the facts of two borderline cases, *Sony Computer Entertainment America Inc. v. Gamemasters*²⁰⁰ and *Davidson & Associates, Inc. v. Internet Gateway*.²⁰¹ The foregoing analysis illustrates that the *Chamberlain* test effectively distinguishes between durable goods and digital content products in finding liability.

A. Chamberlain Test Applied to *Lexmark v. Static Control*

Like *Chamberlain*, *Lexmark* involved the sale of after-market goods that circumvented an authentication sequence measure in order to interoperate with a product containing a copyrighted computer program. Because of the similarity of the two cases, application of the *Chamberlain* test to the facts of *Lexmark* serves as a useful check on the test’s effectiveness.

Under the *Chamberlain* test, the plaintiff must first prove ownership of a valid copyright on a work. The Sixth Circuit concluded that the Toner Loading Program contained on the toner cartridge lacked originality and thus was not copyrightable;²⁰² however, the parties agreed that the Printer Engine Program was copyrightable.²⁰³ Since the copyright of the Printer Engine Program was not contested, this element of the *Chamberlain* test would be satisfied as to that program.

Second, the plaintiff must prove that the copyrighted work is effectively controlled by a technological measure, which has been circumvented. The court in *Chamberlain III* did not address the meaning of “effectively.”²⁰⁴ The court in *Lexmark II* concluded that the “SMARTEK” micro-

¹⁹⁹ *Id.* at 1204.

²⁰⁰ 87 F. Supp. 2d 976 (N.D. Cal. 1999).

²⁰¹ 334 F. Supp. 2d 1164 (E.D. Mo. 2004), *aff’d sub nom.* *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005).

²⁰² *Lexmark II*, 387 F.3d 522, 544 (6th Cir. 2004).

²⁰³ *Id.* at 546.

²⁰⁴ As discussed *supra*, the term can mean either “in effect” or “successfully.” [WHERE]

chip did circumvent the authentication sequence, but that the authentication sequence did not control all access to the Printer Engine Program.²⁰⁵ Because the authentication sequence “in effect” blocked access but did not do so completely, this element would only be satisfied under a broad interpretation of the term “effectively.”

Third, the plaintiff must prove that the circumvention of the authentication sequence resulted in third parties being able to “now access” the copyrighted program. As discussed above, the phrase “can *now* access” in the *Chamberlain* test is ambiguous. On one hand, the phrase could be construed broadly to mean only that some means of access was previously blocked by the technological measure that is now rendered ineffective because of the circumvention. On the other hand, the phrase could be interpreted narrowly to mean that the copyrighted material is now accessible by circumvention where it was not at all accessible before, either by the means of access controlled by the technological measure or by any other means. In *Lexmark II*, the court noted that the Printer Engine Program could be accessed without circumventing the authentication sequence, since the program was not encrypted and so could be decompiled to obtain the source code.²⁰⁶ Interpreting the phrase “now access” as implying the lack of any access prior to circumvention would incorporate the reasoning from *Lexmark II* with respect to the *effectiveness* of the technological control. Since the authentication sequence did not control *all* access to the Printer Engine Program, third parties cannot “now access” the program because they could already access it before the circumvention. Accordingly, this element would only be satisfied under a broad interpretation of the phrase “can now access.”

Fourth, the plaintiff must prove that the access was without authorization. In *Lexmark II*, the consumers agreed via shrinkwrap license not to use third party toner cartridges with the Lexmark printer.²⁰⁷ To the extent the shrinkwrap license is enforceable, it means that the consumers were not authorized to use an after-market toner cartridge containing a circumvention microchip in order to gain access to the copyrighted Printer Engine Program. Of course, the shrinkwrap license would not affect the consumers’ right to access and decompile the unencrypted Printer Engine Program without circumvention, unless the license expressly stated that purchasers of Lexmark printers could not do so. Nevertheless, with respect to the circumvention device, this element of the test would be satisfied.

Fifth, the plaintiff must prove that the circumvention of the technological measure was in a manner that infringed or facilitated infringement of the copyrighted Printer Engine Program. In *Lexmark II*, there was no evidence that the authentication sequence was circumvented in order to infringe the

²⁰⁵ *Lexmark II*, 387 F.3d. at 546–47.

²⁰⁶ *See id.* at 547.

²⁰⁷ *Id.* at 530.

copyright of the Printer Engine Program.²⁰⁸ Moreover, there was no evidence that the circumvention facilitated infringement of the program by a third party.²⁰⁹ Rather, the circumvention was carried out to make the after-market cartridge interoperate with the Lexmark printer.²¹⁰

Because Lexmark would be unable to prove the existence of a “reasonable relationship” between access and infringement as embodied in element (5), the plaintiff’s claim of violation under § 1201(a)(2) must fail. As such, the sixth element of the *Chamberlain* test need not be considered.²¹¹ This result is consistent with the Sixth Circuit’s actual holding in *Lexmark II* and is also consistent with the intent of Congress to create a new type of liability and not a new property right over durable goods incorporating copyrighted material.

B. Chamberlain Test Applied to Sony v. Gamemasters

In *Sony Computer Entertainment America Inc. v. Gamemasters*,²¹² the plaintiff manufactured PlayStation, “an electronic game system designed to allow users to play CD-Rom video games at home on a television.”²¹³ The PlayStation computer program contained a mechanism (an access control measure) that allowed the program to access only those games with data codes that matched the geographical location of the game console itself.²¹⁴ The defendants owned a retail shop that sold a device called a “Game Enhancer.”²¹⁵ The Game Enhancer device permitted users in the United States to play imported (nonterritory) games, which were intended by Sony for use exclusively on the corresponding non-U.S.-market PlayStation consoles.²¹⁶

The plaintiffs argued that the Game Enhancer could be used not only to play legitimately purchased import (nonterritory) games on a U.S. PlayStation console, but to play counterfeit copies of PlayStation games.²¹⁷ The plaintiffs alleged contributory copyright infringement and violation of the anticircumvention provisions of the DMCA.²¹⁸

²⁰⁸ *Id.* at 548. Specifically, the Printer Engine Program was not copied or used to create derivative works, rather it was simply used. *Id.*

²⁰⁹ *Id.* at 553.

²¹⁰ *Id.*

²¹¹ The evidence in *Lexmark II* showed that Static Control designed the SMARTEK chip primarily to circumvent the authentication sequence, that the chip had only limited commercial significance other than circumvention, and that the chip was marketed for use in circumventing the authentication sequence. *Id.*

²¹² 87 F. Supp. 2d 976 (N.D. Cal. 1999).

²¹³ *Id.* at 979.

²¹⁴ *Id.* at 981.

²¹⁵ *Id.* at 978, 981.

²¹⁶ *Id.* at 981.

²¹⁷ *Id.* at 982.

²¹⁸ *Id.* at 978.

On a motion for preliminary injunction, the Northern District of California found that the evidence showing the Game Enhancer was used to play counterfeit games was insufficient to support a claim of contributory infringement.²¹⁹ However, the court issued a preliminary injunction against GameMasters based upon a violation of § 1201(a)(2).²²⁰ The court concluded that the primary function of the Game Enhancer was to circumvent a mechanism on Sony's PlayStation game console that prevented users from playing imported Sony video games and that this circumvention constituted a DMCA violation.²²¹

As discussed above, according to the *Chamberlain* test the plaintiff must prove six elements to establish a prima facie case of violation of § 1201(a)(2) of the DMCA. First, the plaintiff must prove ownership of a valid copyright on a work. In *Sony*, the defendant did not dispute that the plaintiff owned a valid copyright for its PlayStation games, and instead asserted copyright misuse as a defense.²²² Accordingly, this element of the *Chamberlain* test was easily satisfied.

Second, the plaintiff must prove that the copyrighted work is effectively controlled by a technological measure, which has been circumvented. The court in *Sony* ruled on the DMCA claim based on the use of the Game Enhancer to allow users to play games sold for a non-U.S. territory on U.S. PlayStation consoles.²²³ The PlayStation authentication sequence ordinarily prevented games sold in non-U.S. markets from playing on U.S. PlayStation consoles.²²⁴ Thus, the authentication sequence was as a technological measure that controlled *access* to those games.²²⁵ The technological measure also was circumvented; one of the functions of the Game Enhancer was to circumvent the authentication sequence and “trick” the PlayStation into accepting a foreign-origin CD ROM as if it were authorized.²²⁶ The court in *Sony* did not address whether the authentication sequence was *effective*. As in *Lexmark*, the copyrighted game software could be accessed without circumvention by simply playing the game on a PlayStation sold to the corresponding market. Thus, because the authentication sequence did not block *all* access to the game, this element would only be satisfied under a broad interpretation of the term “effectively.”

Third, the plaintiff must prove that the circumvention of the authentication sequence resulted in third parties being able to “now access” the copyrighted program. As discussed above, the PlayStation game software could

²¹⁹ *Id.* at 987.

²²⁰ *Id.* at 988.

²²¹ *Id.* at 987.

²²² *Id.* at 988–89.

²²³ *Id.* at 987–88.

²²⁴ *Id.* at 987.

²²⁵ *Id.*

²²⁶ *Id.* at 981.

be accessed by a means not involving circumvention of the authentication sequence (i.e., by using the corresponding non-U.S. PlayStation console). Thus, if the phrase “now access” is interpreted to imply that access was not possible by any means prior to circumvention, this element would not be satisfied. Nevertheless, this element would be satisfied under a broad interpretation of the phrase “now access” because a game purchased in a non-U.S. market could not be played on a U.S. PlayStation console without using the defendant’s device to circumvent the authentication sequence (i.e., this particular means of access was not previously available).

Fourth, the plaintiff must prove that the access was unauthorized. The district court’s opinion in *Sony* does not state that the sale of the PlayStation game included an enforceable shrinkwrap license whereby a legitimate purchaser of a game was expressly prohibited from accessing that game with an unauthorized player.²²⁷ Absent such a shrinkwrap license, a legitimate purchaser should be authorized to access the game however he wants—either because of an implied authorization, the first-sale doctrine, or both. Thus, the plaintiffs would only be able to satisfy this element if they could prove the existence of a binding license containing an express prohibition.²²⁸

Fifth, the plaintiff must prove that the circumvention of the technological measure was in a manner that infringed or facilitated infringement of the copyrighted PlayStation game software. The court in *Sony* concluded that there was insufficient evidence to support the plaintiff’s charge that the Game Enhancer facilitated the sale of counterfeit or pirated games.²²⁹ Certainly if the plaintiff could make a sufficient showing that the Game Enhancer was used to *produce* counterfeit games, then this element would be satisfied. The mere fact that counterfeit games could be played using the Game Enhancer does not mean that the Game Enhancer facilitated infringement insofar as the act of infringement (the illegal copying of the game) was wholly separate from the use of the Game Enhancer. Thus, absent such a showing, the plaintiff would have to establish that use of the Game Enhancer to play non-U.S. market games on a U.S. market PlayStation facilitated infringement of a copyright.

Since there did not appear to have been any license agreement expressly prohibiting legitimate purchasers of PlayStation games from playing their games on PlayStation consoles from other territories, circumvention of the access control measure could not be “in a manner that infringed or facilitated infringement” as required by the *Chamberlain* test. Accordingly,

²²⁷ *Id.* Shrinkwrap licenses are the licenses that typically accompany a piece of software and state that if you open the shrinkwrap or break the seal on the software envelope you are bound by the terms of the license, whether or not you had the chance to read the whole agreement. See, e.g., Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1241 (1995).

²²⁸ Proving the existence of a binding license with restrictive terms (such as zoning restrictions) is difficult because such terms would be unenforceable in many foreign jurisdictions.

²²⁹ *Sony*, 87 F. Supp. 2d at 986–87.

although the court in *Sony* did conclude that the Game Enhancer was designed primarily to circumvent the authentication sequence,²³⁰ the plaintiff's claim would fail on the basis of this "reasonable relationship" element.²³¹ Significantly, this result is contrary to the district court's holding in *Sony*, suggesting that the *Chamberlain* test, if applied to a similar set of facts in the future, would produce a result more in line with the legislative intent to prevent copyright infringement rather than to restrict the right of game owners to use their property as they wish.²³²

C. Chamberlain Test Applied to Davidson v. Internet Gateway

Davidson & Associates, Inc. v. Internet Gateway presented facts that involved the circumvention of a "secret handshake" authentication sequence.²³³ In *Davidson*, the plaintiffs (referred to as Blizzard) operated an Internet-based gaming service called "Battle.net" that provided purchasers of its computer games with free game-enhancing features.²³⁴ The defendants developed their own online gaming service called "BnetD," which emulated all the functions and features of Battle.net and could be used with Blizzard computer games.²³⁵ In order to make the BnetD server interact with Blizzard's computer game software, the defendants had to reverse engineer the protocol language Blizzard used in its games so that it could be used on the BnetD server.²³⁶

Blizzard owned valid copyright registrations for the Battle.net gaming server program and each of the Blizzard computer games.²³⁷ The copyrighted computer games were not protected by any sort of encryption.²³⁸ Instead, Blizzard required the user to enter a "CD Key" (a rights control measure) before a game could be installed on a personal computer.²³⁹ The user also needed to satisfy an authentication sequence (an access control

²³⁰ *Id.* at 987.

²³¹ The court noted that the customer's choice to play an imported authentic Sony game cannot be infringing Sony's copyright since the games were legally manufactured and sold in Japan. *Id.* at 986.

²³² Of course if there had been a license agreement expressly prohibiting legitimate purchasers of PlayStation games from playing their games on PlayStation consoles from other territories, then the circumvention might be considered to facilitate infringement because it would facilitate access in contravention of the license agreement.

²³³ 334 F. Supp. 2d 1164 (E.D. Mo. 2004), *aff'd sub nom.* Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005).

²³⁴ *Id.* at 1168. Such features included multiplayer gaming options, private chat channels, a means of recording wins and losses, a means of creating individual game accounts, and the opportunity to participate in tournaments. *Id.*

²³⁵ *Id.* at 1172.

²³⁶ *Id.*

²³⁷ *Id.* at 1168.

²³⁸ *Id.* at 1169 (stating that the "games can be easily copied and distributed over the Internet").

²³⁹ Second Amended Complaint at 20, Davidson & Assocs., Inc. v. Internet Gateway, 334 F. Supp. 2d 1164 (E.D. Mo. 2004) (No. 4:02-CV-498-CAS), available at http://www.eff.org/IP/Emulation/Blizzard_v_bnetd/20021203_SAC.pdf [hereinafter Second Amended Complaint].

measure) in order to validate and verify the uniqueness of the CD Key before he could access Battle.net.²⁴⁰ Once the game was installed, the game could be played either by a single player or with other players via a local area network (“LAN”), direct computer connections, or the Battle.net server.²⁴¹ The defendant’s gaming service (BnetD) functioned in the same way as the Blizzard gaming service (Battle.net) except that it did not evaluate the validity or uniqueness of a game’s CD Key before allowing the user to access and use the service (i.e., BnetD did not use an access control measure).²⁴²

Blizzard alleged that the defendants’ development of the BnetD gaming service, which did not verify whether users had a legitimate copy of the Blizzard game, violated § 1201(a)(1)(A) and (a)(2) of the DMCA because the defendants’ gaming service was a “technology” that “circumvented” Blizzard’s access control measure in order to allow players to gain “unauthorized access” to Blizzard games in Battle.net mode (i.e., with all the additional features and functions).²⁴³ The court held on a motion for summary judgment that the defendants’ actions constituted a violation under § 1201(a)(1)(A) and (a)(2).²⁴⁴ The Eighth Circuit affirmed on appeal, but notably did not apply the *Chamberlain* test.²⁴⁵

Although there are significant issues in the *Davidson* case related to the defendants’ interoperability defense,²⁴⁶ the analysis here will focus only on whether Blizzard would have a prima facie case under § 1201 if the *Chamberlain* test were applied. The parties agreed that Blizzard owned a valid copyright in its games,²⁴⁷ thereby satisfying the first element of the test. Regarding the second element, Blizzard asserted that the CD Key and a related authentication sequence constituted a “technological measure” that “controlled access” to its copyrighted games and that the defendants’ BnetD server circumvented that technological measure.²⁴⁸

Before further addressing whether the technological measure “effectively” controlled access, it is important to assess what the authentication sequence actually protected. If Abe bought a Blizzard game and gave Bob an unauthorized copy of it along with Abe’s CD Key, both Abe and Bob could each: (1) play the game on their own computers against a computer opponent, (2) play the game against each other via a LAN or modem con-

²⁴⁰ *Davidson*, 334 F. Supp. 2d at 1169.

²⁴¹ Second Amended Complaint, *supra* note 239, at 5.

²⁴² *Davidson*, 334 F. Supp. 2d at 1173.

²⁴³ The games could be played in “Battle.net” mode through the BnetD server. Blizzard also alleged that defendants distributed the BnetD emulator knowing that it could be used to circumvent Blizzard’s technological controls. *See id.* at 1183; Second Amended Complaint, *supra* note 239, at 15–16.

²⁴⁴ *Davidson*, 334 F. Supp. 2d at 1184–85.

²⁴⁵ *Davidson & Associates v. Jung*, 422 F.3d 630 (8th Cir. 2005).

²⁴⁶ *Davidson*, 334 F. Supp. 2d at 1183–87.

²⁴⁷ *Id.* at 1168.

²⁴⁸ Second Amended Complaint, *supra* note 239, at 7, 15–16.

nection, or (3) play the game using Battle.net mode provided they do not logon to Battle.net at the same time.²⁴⁹ All three options would be available without circumventing the authentication sequence. If Cal purchased a pirated copy of a game off the Internet but didn't have a CD Key, Cal would not be able to install his game, play the game on his own computer, or access Battle.net mode because he would be blocked by the rights control measure (the CD Key protection measure). If Cal managed to circumvent the rights control measure and install the game without the CD Key, he would be able to play his game on his computer but would remain unable to use Battle.net mode without circumventing the authentication sequence. Thus, the authentication sequence protected only some aspects of the access to the copyrighted work. However, because the authentication sequence did completely control access to Battle.net mode with respect to those aspects, it "effectively" controlled access in those circumstances even under the more restrictive interpretation of "effectively."

The third element of the *Chamberlain* test requires that third parties "can now access" the copyrighted work. Although some parties could previously access Blizzard's copyrighted game on their computers (because they had either a legitimately purchased or pirated game copy with a CD Key), in certain cases access to Blizzard's Battle.net mode was prevented (Abe and Bob cannot play each other in Battle.net mode and Cal cannot play at all in Battle.net mode). The defendant's BnetD server allowed parties to access advanced features similar to those found in Battle.net mode, which they could not previously access. However, the advanced features now accessible through the BnetD server are not subject to a copyright owned by Blizzard. Rather the advanced features now accessible through the BnetD server are merely a reverse-engineered copy of Blizzard's copyrighted software. While the defendants' act of reverse engineering Blizzard's internet game server may itself be a copyright violation, such an act is wholly independent of the access provided by the BnetD server. Accordingly, the third element was not satisfied because the access now available is not access to a copyrighted work owned by Blizzard.

The fourth element requires proof that the access was without authorization. This element was likely satisfied because the click-wrap license clearly stated that the defendants did not have authorization from Blizzard to circumvent the authentication sequence in order to gain access to the advanced game features of Battle.net mode, assuming the click-wrap license was enforceable in that respect.²⁵⁰

The fifth element is whether the BnetD server circumvents the authentication sequence in a way that infringes or facilitates infringement. As discussed above, the BnetD server circumvented the authentication sequence,

²⁴⁹ If Abe and Bob logged onto Battle.net at the same time, the authentication sequence would refuse the second user because the CD Key was already in use.

²⁵⁰ *Davidson*, 334 F. Supp. 2d at 1170-71.

which in certain situations completely controlled access to the online advanced game features of Battle.net mode. However, in these situations, the circumvention was not reasonably related to copyright infringement because although it allowed the gamer to play a pirated game in a way that was otherwise inaccessible (using advanced online game features), it did not provide access to any of Blizzard's copyrighted works to which the users did not already have access. Rather, the BnetD server provided access to BnetD advanced game features. Accordingly, it would appear that the plaintiff should have been unable to satisfy this element of the *Chamberlain* test.

Even if the plaintiff could establish each of the first five elements, the plaintiff would still need to demonstrate that 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.²⁵¹

In *Davidson*, the defendants did not dispute Blizzard's allegations that all three of these criteria had been met,²⁵² even though it seems that the defendants may have had grounds to challenge Blizzard's assertions, especially considering the standard on summary judgment.²⁵³ The sixth element of the test relates to the defendant's intent and purpose in developing the circumvention software. Here the defendants did not design the BnetD server in order to circumvent Blizzard's access control measure and allow gamers with pirated game copies to access Blizzard's copyrighted Battle.net mode (an act that would be a classic case of facilitating piracy). Rather, the defendants' purpose was to create an independent, alternative game server that could provide similar enhanced features to those found on the Battle.net server (recreated from the Battle.net server through reverse engineering) but without the alleged problems.

Applying the *Chamberlain* test to the facts of *Davidson v. Internet Gateway* produces a result that is at odds with the Eighth Circuit's recent decision affirming DMCA liability. Notably the Eighth Circuit did not apply the *Chamberlain* test, or even cite to the *Chamberlain* decision. In this case, the *Chamberlain* test appears to provide a result that is consistent with the legislative intent insofar as it finds no liability for defendants whose "circumvention" does not facilitate copyright infringement. Accordingly,

²⁵¹ See *supra* notes 132–133 and accompanying text.

²⁵² *Davidson*, 334 F. Supp. 2d at 1186.

²⁵³ See *id.* at 1185–86 (discussing the three tests for liability). Surely there was a question of fact as to these elements. For example, although the evidence suggests the BnetD server was primarily designed to provide an alternative environment in which users could play their games, there is no evidence the primary purpose was to circumvent the "secret handshake." Moreover, there is little evidence that there was any commercially significant purpose at all insofar as the BnetD server program was open source. Finally, there is no evidence that the defendants marketed the BnetD server as a means for circumventing the "secret handshake" authentication sequence.

the *Chamberlain* test proves to be a workable test for determining liability under § 1201(a)(2) of the DMCA.

V. THE FUTURE OF THE DMCA

The Federal Circuit's decision in *Chamberlain III* provides a useful framework for determining liability under § 1201(a)(2) of the DMCA, and that framework may allay fears that manufacturers could misuse the DMCA to improperly extend their monopolies. Nonetheless, important issues remain unresolved. In particular, the scope of the fair use doctrine and other copyright law exemptions under the DMCA remains unclear. The Federal Circuit's dicta raises questions relating to whether a copyright owner can, by contract, override the fair use and other rights of a public user of a copyrighted work.²⁵⁴

In both *Chamberlain III*²⁵⁵ and *Lexmark II*,²⁵⁶ the defendants raised the fair use defense of interoperability under § 1201(f). However, neither appellate court based its judgment upon a statutory exception. Rather, the courts construed § 1201(a)(2) in a way that rendered the elements required for a prima facie case of liability not satisfied, thereby obviating the need to consider fair use defenses. Accordingly, the appellate courts' decisions in these cases do not provide any definitive answers regarding the scope of the "fair use" and other copyright use exemptions of the DMCA. Nevertheless, within the courts' opinions in *Chamberlain III* and *Lexmark II*, there is dicta that may be encouraging to public users of copyrighted materials.

For example, although the Federal Circuit in *Chamberlain III* did not address Skylink's interoperability defense directly, the court did make some statements suggesting that fair use and other copyright use exemptions to the DMCA might exist. Specifically, the court acknowledged that there was a "significant difference" between defendants whose devices "enable copying" and defendants whose devices "enable only legitimate uses."²⁵⁷ Also, the court rejected a construction of the statute that would have allowed copyright owners to "block *all* access" to their copyrighted works because such a construction would conflict with § 1201(c)(1), the lone section of the DMCA which suggests that fair use and other copyright use exemptions may be a valid defense to liability under the DMCA.²⁵⁸ However, the court further suggested that Congress knowingly prohibited some non-

²⁵⁴ Although § 1201(c)(1) provides that § 1201 does not affect traditional defenses to copyright infringement, including fair use, courts have ruled that fair use is not a defense to a circumvention offense under the DMCA. See Band, *supra* note 25.

²⁵⁵ *Chamberlain III*, 381 F.3d 1178, 1186 & n.5 (Fed. Cir. 2004) (describing Skylink's defense that its activities fell under the interoperability exception of § 1201(f)).

²⁵⁶ *Lexmark II*, 387 F.3d 522, 550 (6th Cir. 2004).

²⁵⁷ *Chamberlain III*, 381 F.3d at 1198.

²⁵⁸ *Id.* at 1199 ("[N]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." (quoting 17 U.S.C. § 1201(c)(1) (2000)).

infringing public uses because such sacrifice was necessary in order to achieve an overall balance between the interests of copyright owners and public users of copyright materials.²⁵⁹

In *Lexmark II*, the Sixth Circuit held that the plaintiff had failed to establish a claim of liability under § 1201(a)(2) but nevertheless elected to comment on Static Control's interoperability defense.²⁶⁰ According to § 1201(f)(3), a defendant is not liable under § 1201(a)(2) for making information acquired in violation of the statute available to others as long as the violation was for the purpose of enabling interoperability of an independently created computer program with other programs and such means were necessary to achieve interoperability.²⁶¹ The district court in *Lexmark I* rejected this defense on the basis that Static Control's "SMARTEK" microchip could not be considered to contain an independently created computer program.²⁶² The Sixth Circuit disagreed and stated that Static Control could benefit from the interoperability defense.²⁶³ In response to Lexmark's argument that the independent programs must exist prior to the "reverse engineering," the court clarified that the statute does not preclude simultaneous creation of an interoperability device and another program.²⁶⁴ Lexmark also argued that the technological means that were reverse engineered must be "necessary or absolutely needed"; the court responded that the statute was silent about the degree to which the means must be necessary if necessary at all.²⁶⁵

Therefore, the Federal Circuit and Sixth Circuit seemed to acknowledge that fair use defenses to the DMCA exist, although the *Chamberlain III* court suggested that the scope of the fair use defense to violations of the DMCA may be narrower than the corresponding scope of the fair use defense to copyright infringement.²⁶⁶ Significantly, the court in *Lexmark II* concluded that Static Control's defense was at least sufficient to survive preliminary injunction.²⁶⁷

It is important to note that the courts' statements in *Chamberlain III* and *Lexmark II* contrast sharply with those of the Second Circuit in *Universal City Studios, Inc. v. Corley*.²⁶⁸ In *Universal City Studios*, the Second

²⁵⁹ *Id.* at 1198 (arguing that sacrificing some public uses was necessary in order to rebalance the interests).

²⁶⁰ *Lexmark II*, 387 F.3d at 550.

²⁶¹ 17 U.S.C. § 1201(f)(3).

²⁶² *Lexmark II*, 387 F.3d at 550.

²⁶³ The Sixth Circuit disagreed with the district court's conclusion because it felt the district court had improperly rejected testimony that the microchip contained other functional programs beyond the copied Toner Loading Program. *Id.*

²⁶⁴ *Id.* at 550–51.

²⁶⁵ *Id.*

²⁶⁶ See *Chamberlain III*, 381 F.3d 1178, 1198 (Fed. Cir. 2004).

²⁶⁷ *Lexmark II*, 387 F.3d at 550.

²⁶⁸ *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

Circuit asserted that § 1201(c)(1) of the DMCA did not provide an exception to liability when circumvention was carried out for fair use purposes, but merely ensured that the DMCA was not “read to prohibit the ‘fair use’ of information just because that information was obtained in a manner made illegal by the DMCA.”²⁶⁹ In rejecting the argument that fair use was constitutionally required, the court stated that fair use under the Copyright Act was not a “guarantee,” that fair use could be carried out using the optimal method, or that a “fair user” was entitled to an identical copy.²⁷⁰ Thus, unlike the Federal Circuit and Sixth Circuit, the Second Circuit did not consider fair use to be a defense to liability under the DMCA.²⁷¹

VI. CONCLUSION

The problem with the DMCA’s access control provisions is that they fail to distinguish what the access mechanism protects, i.e., whether it protects a copyrighted work from infringement or a device from being used with third-party, after-market hardware. By interpreting the DMCA as requiring access to be “reasonably related” to copyright infringement, the Federal Circuit has addressed some of the criticisms of the DMCA by prohibiting manufacturers from profiting from copyright misuse. However, the Federal Circuit’s opinion in *Chamberlain III* only covers a situation where circumvention is incapable of facilitating infringement; the application of the DMCA in a situation where circumvention facilitates both infringing and noninfringing uses remains an open question. Moreover, in light of the conflicting views of the different appellate courts, the question of the fair use defense under the DMCA remains unclear. Nevertheless, the *Chamberlain* test is a workable framework for determining liability and a significant first step toward resolving the many criticisms of the DMCA.

²⁶⁹ *Id.* at 443.

²⁷⁰ *Id.* at 459 (“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.”).

²⁷¹ *Id.*