Daniel Higgs December 19, 2003

Law and Technology Writing Workshop

FINAL DRAFT

EVALUATING THE EXTENSION OF THE DMCA TO DURABLE GOODS AFTERMARKETS: *LEXMARK INTERNATIONAL, INC. V. STATIC CONTROL COMPONENTS, INC.* & *CHAMBERLAIN GROUP, INC. V. SKYLINK TECHNOLOGIES, INC.*

The advent of the Internet brought with it the specter of digital piracy. Infringers had at their disposal an efficient means for replicating and distributing copyrighted works. Concerned by this prospect, content industries, such as software and movie companies, began protecting their works via encryption and other digital techniques.[1] However, these protective measures were subject to circumvention.[2] The content industries thus requested that the government create legal defenses for their digital safeguards.[3]

Congress responded by enacting the Digital Millennium Copyright Act ("DMCA," or "the Act")[4] in 1998. Among other things, the DMCA contains the so-called anti-circumvention provisions, which prohibit the acts of circumventing and trafficking in devices that circumvent technological measures designed to protect copyrighted works from unauthorized access or use.[5] But while these broad prohibitions function as the shield that the content industries desired, unrelated industries have wielded them as a sword.[6]

In two recent cases, manufacturers of durable goods used the DMCA in an attempt to stifle competition in the aftermarket setting. In *Lexmark International, Inc. v. Static Control*

---

[1] *See* Peter S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63, 134 (2003).
[2] *See* INFORMATION INFRASTRUCTURE TASK FORCE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY RIGHTS AND THE NATIONAL INFORMATION INFRASTRUCTURE 230 (Sept. 1995), *at* http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf ("[T]echnology can be used to defeat any protection that technology may provide.").
[3] *See* Menell, *supra* note 1, at 133.
[4] Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 5, 17, 28, and 35 U.S.C.).
[5] 17 U.S.C. §§ 1201(a)–1201(b) (2002). For an in-depth analysis of the anti-circumvention provisions, *see, e.g.*, Nimmer § 12A.03.
[6] *See* Dan Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1135-36 (2003).

Components, Inc.,[7] a laser printer manufacturer sued a supplier of toner cartridge refurbishing equipment under the DMCA, seeking to enjoin the manufacture and marketing of a microchip that enabled unauthorized toner cartridges to work in the plaintiff's printers by circumventing an authentication sequence. Similarly, in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*,[8] a garage door opener manufacturer invoked the DMCA in an attempt to prevent a competing company from selling replacement transmitters.

This Note explores the legitimacy of these new applications of the DMCA's anti-circumvention provisions. Part I outlines the legal and economic contexts in which these new cases arise. Part II details the *Lexmark* and *Chamberlain* cases, both of which diverge from the archetypal application of the DMCA, yet represent foreseeable efforts to extend the Act's reach in light of the economics of aftermarkets. Part III evaluates whether the DMCA should be revised in order to prevent this apparently unintended application of the law. This Note concludes that no such revision is required because courts may determine this new application to be inconsistent with legislative intent, they may accept the equitable defense of misuse in the paracopyright realm, and the Act already contains exceptions for this type of case.

I. LEGAL AND ECONOMIC BACKGROUND

It is necessary to first describe the legal landscape in which the *Lexmark* and *Chamberlain* cases lie in order to later demonstrate their apparent incongruity in this setting. This section shows that the development of the DMCA's anti-circumvention provisions and their subsequent application in the courts deal almost exclusively with the interests of content industries—namely, movie studios, book publishers, software developers, and music companies. Durable goods manufacturers and aftermarket industries were absent in the hearings and debates

[7] 253 F. Supp. 2d 943 (E.D. Ky. 2003).
[8] No. 02 C 6376, 2003 WL 22038638 (N.D. Ill. Aug. 29, 2003); No. 02 C 6376, 2003 WL 22697217 (N.D. Ill. Nov. 13, 2003).

that shaped these provisions. Therefore, to provide background for the extension of the DMCA into this unrelated field, this section concludes with a description of aftermarket economics.

A. Development of the DMCA's Anti-Circumvention Provisions

In 1993, the Clinton Administration assembled the Information Infrastructure Task Force to contend with the effects of emerging digital technologies on intellectual property.[9] The task force conducted hearings at which content industries played a dominant role.[10] It then issued the White Paper—a report that proposed drastic changes to the Copyright Act.[11] One proposed change, which was chiefly inspired by the motion picture industry,[12] would have outlawed devices designed primarily to circumvent "copyright protection systems."[13] This proposal was prompted by the fear that digital piracy would dissuade content industries from marketing their products over the Internet.[14] The 104th Congress considered the suggestions set forth in the White Paper, but efforts to adopt new legislation ultimately failed.[15]

Shortly thereafter, the White Paper's proposals resurfaced in an international setting. At the 1996 diplomatic conference held by the World Intellectual Property Organization (WIPO) in Geneva, the U.S. delegation, realizing that the global reach of the Internet made digital piracy an

---

[9] S. REP. NO. 105-190, at 2 (1998).
[10] *Id. See also* JESSICA LITMAN, DIGITAL COPYRIGHT 90-95 (2001).
[11] *See* Pamela Samuelson, *The Copyright Grab* (Jan. 1996), *at* http://www.wired.com/wired/archive/4.01/white.paper_pr.html.
[12] *See* Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369, 410 (1997).
[13] *See* INFORMATION INFRASTRUCTURE TASK FORCE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY RIGHTS AND THE NATIONAL INFORMATION INFRASTRUCTURE, app. 1 at 6 (Sept. 1995), *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf. The proposed legislation reads:

> § 1201. Circumvention of Copyright Protection Systems
> No person shall import, manufacture or distribute any device, product, or component incorporated into a device or product, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent, without the authority of the copyright owner or the law, any process, treatment, mechanism or system which prevents or inhibits the violation of any of the exclusive rights of the copyright owner under section 106.

Id.
[14] *Id.* at 10.
[15] S. REP. NO. 105-190, at 4 (1998).

international problem, proposed anti-circumvention measures similar to those found in the White Paper.[16] U.S. content industries also played a major role at this international stage.[17]

The U.S. measure as proposed failed, but less imposing provisions were adopted in both the WIPO Copyright and WIPO Performances and Phonograms Treaties.[18] These provisions required that participating countries "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures" used to protect copyrighted works.[19] A fundamental goal of the WIPO treaties was "to maintain a balance between the rights of authors and the larger public interest."[20]

Although U.S. copyright law arguably already provided sufficient protection and remedies to satisfy the standards adopted in the two WIPO treaties,[21] the content industry lobbied for greater protection.[22] Congress thus considered legislation for implementing the treaties that would include more expansive anti-circumvention provisions than those proposed in the White

[16] *See* Samuelson, *supra* note 12, at 410-14.
[17] *See* David Nimmer, *Time and Space*, 38 IDEA 501, 508-10 (1998) (stating that a disproportionate number of non-governmental organizations at the WIPO convention were of U.S. origin, and that the "world of copyright is now dancing to an American tune"); *see also* WIPO, Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, List of Participants, 55-66, http://www.wipo.org/documents/en/diplconf/distrib/msword/inf2.doc.
[18] *See* Samuelson, *supra* note 12, at 414-15.
[19] WIPO Copyright Treaty, art. 11, adopted Dec. 20, 1996, *at* http://www.wipo.int/clea/docs/en/wo/wo033en.htm; WIPO Performances and Phonograms Treaty, art. 18, adopted Dec. 20, 1996, *at* http://www.wipo.int/clea/docs/en/wo/wo034en.htm.
[20] WIPO Copyright Treaty, preamble, adopted Dec. 20, 1996, *at* http://www.wipo.int/clea/docs/en/wo/wo033en.htm; WIPO Performances and Phonograms Treaty, preamble, adopted Dec. 20, 1996, *at* http://www.wipo.int/clea/docs/en/wo/wo034en.htm.
[21] *See, e.g.*, Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 530-34 (1999) ("The [WIPO anti-circumvention norm] was, after all, very general in character and provided treaty signatories with considerable latitude in implementation…. The U.S. could have pointed to a number of statutes and judicial decisions that establish anti-circumvention norms. With U.S. copyright industries thriving in the current legal environment, it would have been fair to conclude that copyright owners already were adequately protected by the law."). *But see* 3 NIMMER ON COPYRIGHT § 12A.01 (2002) (stating that the *Sony* standard for legalizing technologies "capable of a commercially significant noninfringing use" gave insufficient protection under the WIPO treaties, thus requiring the U.S. to adopt new legislation).
[22] *See* Samuelson, *supra* note 21, at 533-34.

Paper.[23] Congress eventually enacted these provisions as part of the DMCA, and intended them to "create the legal platform for launching the global digital online marketplace for copyrighted works."[24]

B. The DMCA Anti-circumvention Provisions: § 1201

Congress crafted the DMCA anti-circumvention measures as a set of blanket prohibitions tempered by several narrow exceptions. These prohibitions give copyright owners rights in addition to and independent from those that inhere in a copyrighted work.[25] As a result, some have dubbed the interests protected by the anti-circumvention provisions "paracopyright."[26]

The primary prohibition set forth in § 1201 is against the act of "circumvent[ing] a technological measure that effectively controls access to a work protected under [the Copyright Act]."[27] This prohibition thus creates a new "right of access" in certain copyrighted works.[28] In explaining this right, Congress adopted the analogy of breaking into a locked room to obtain a copy of a book; it is the act of breaking in, rather than the subsequent use of the book, that is prohibited.[29]

The statute defines the language of this first prohibition: "[T]o 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure without the authority of the copyright owner."[30] The statute also clarifies what is meant for a technological measure to "effectively control[] access to a work," again emphasizing the crucial role of the

---

[23] *See id.* at 531-34; *see also* Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1634 (2002).
[24] S. REP. NO. 105-190, at 2 (1998).
[25] *See* 3 NIMMER ON COPYRIGHT § 12A.18[B], at 12A-186 (2002).
[26] *Id.*
[27] 17 U.S.C. § 1201(a)(1)(A) (2000).
[28] *See* Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium"*, 23 COLUM.-VLA J.L. & ARTS 137, 140-43 (1999).
[29] *See* H.R. REP. NO. 105-551, pt. 1, at 17 (1998).
[30] 17 U.S.C. § 1201(a)(2)(A) (2000).

copyright owner's authority.[31] However, the Act is silent on the meaning of "access," which is the central word of the provision.[32]

The DMCA further prohibits the trafficking of tools used to circumvent two different classes of technological measures: those that control access to a copyrighted work and those that protect "a right of a copyright," such as the right to reproduce or distribute.[33] Software that defeats video game console mechanisms which prevent access to games in unlicensed geographical regions exemplifies the first category of prohibited tools;[34] software that defeats the new "copy-protection" feature on some music CDs exemplifies the second.[35] For either category, the Act dictates that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" that falls into any of three categories: (1) those "primarily designed or produced for the purpose of circumventing" a technological protection measure, (2) those that have "only limited commercially significant purpose or use other than to circumvent" a protection measure, and (3) those marketed for use in such circumvention.[36]

Section 1201 contains seven highly specific exceptions to both the access and anti-trafficking prohibitions, and the scope of the exceptions varies between the two forms of prohibition.[37] In general, there are limited exceptions for libraries and law enforcement agencies, for reverse engineering, encryption research, and security testing activities, and for the protection

---

[31] *Id.* § 1201(a)(2)(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.").
[32] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943, 967 (E.D. Ky. 2003); LITMAN, *supra* note 10, at 144; Samuelson & Scotchmer, *supra* note 23, at 1643-44.
[33] 17 U.S.C. § 1201(a)(2), (b) (2000).
[34] *See* Gamemasters.
[35] *See* ELECTRONIC FRONTIER FOUNDATION, UNINTENDED CONSEQUENCES: FIVE YEARS UNDER THE DMCA 2 (Sept. 24, 2003), *at* http://www.eff.org/IP/DRM/DMCA/unintended_consequences.pdf.
[36] 17 U.S.C. § 1201(a)(2), (b) (2000).
[37] *See* Burk, *supra* note 6, at 1104-05.

of both minors and personal privacy.[38] Furthermore, the DMCA instructs the Librarian of Congress to periodically conduct rulemaking proceedings to exempt legitimate activities from the § 1201(a)(1)(A) prohibition on access control circumvention, but not from liability under the anti-trafficking provisions.[39]

The reverse engineering exception set forth in § 1201(f) is particularly relevant to the present discussion. It provides that one who "lawfully obtain[s] the right to use a copy of a computer program" may circumvent any access controls for the "sole purpose" of achieving interoperability with an "independently created computer program."[40] It further allows for the development of circumvention tools for enabling interoperability and for the distribution of those tools.[41] The statute defines interoperability as "the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged."[42]

C. Cases Interpreting § 1201

Few courts have interpreted the anti-circumvention provisions of the DMCA since its enactment in 1998. However, virtually all cases brought under § 1201 prior to Lexmark filing suit in December 2002 involved content industries,[43] and were thus the type of case

---

[38] 17 U.S.C. § 1201(d)-(j).
[39] *Id.* at § 1201(a)(1)(C)-(E). On October 28, 2003, the Librarian of Congress announced the results of the second rulemaking proceeding. The four additional classes of works that will be subject to exemption from the prohibition in § 1201(a)(1)(A) through October 27, 2006 are: CNET article description – slightly altered.
See Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, *at* http://www.copyright.gov/1201.
[40] 17 U.S.C. § 1201(f)(1).
[41] *Id.* § 1201(f)(2)-(3).
[42] *Id.* § 1201(f)(4).
[43] However, in *PortionPac Chemical Corp. v. Sanitech Systems, Inc.*, 210 F. Supp. 2d 1302 (M.D. Fla. 2002), the plaintiff, a food sanitation service provider, alleged that the defendant, also a food sanitation provider, had violated the DMCA anti-circumvention provisions. The opinion gives an extremely limited presentation of the facts, mainly because the court sustained the defendant's motion to dismiss the DMCA claim: "After looking at the sparse case law on the DMCA, and considering the legislative history behind the Act, the Court finds that the *Digital* Millennium Copyright Act does not allow a cause of action for Plaintiff's claim. As the Fourth Circuit pointed out, '[t]he DMCA was enacted … to preserve copyright enforcement in the Internet.'" *Id.* at 1311-12 (emphasis in

contemplated by Congress when enacting the DMCA.[44] This section briefly outlines some of these pre-*Lexmark* cases.

Sony Computer Entertainment America Inc. v. GameMasters[45] was the first published case interpreting § 1201. In this case, the plaintiff company manufactured PlayStation video game consoles designed to operate only when encrypted data on a game CD verified that the game and console were licensed for the same geographical region.[46] If this authentication procedure failed, the console would not operate the game.[47] The defendant's product allowed PlayStation owners to bypass the authentication procedure and play "non-territorial" games.[48] The court determined that this activity constituted the circumvention of a technological measure designed to control access to copyrighted works.[49] Because this circumvention was the primary purpose of the defendant's product, the court held that the defendant would likely be liable for trafficking in unauthorized devices under § 1201(a)(2)(A) of the DMCA, and issued an injunction.[50]

In *RealNetworks, Inc. v. Streambox, Inc.*,[51] the plaintiff offered software to consumers that enabled Internet streaming of audio and video files encoded in a special digital format.[52] Defendants marketed software that bypassed a "secret handshake" authentication sequence required for accessing these files, and further permitted users to make unauthorized copies of the

---

original) (citation omitted). This case lends further support to the proposition that the DMCA should not be extended beyond its intended purpose. *See infra* Part III.

[44] *See infra* Part III.A.

[45] 87 F. Supp. 2d 976 (N.D. Cal. 1999).

[46] *Id.* at 980.

[47] *Id.* at 981.

[48] *Id.* at 987.

[49] *Id.*

[50] *Id.* at 987, 989-91.

[51] 2000 WL 127311 (W.D. Wash. 2000).

[52] *Id.* at *1. "Streaming" refers to the distribution of an audio or video clip in a format that leaves no trace of the clip on the receiving computer, unless the content owner has additionally permitted downloading. *Id.*

files.[53] The court thus determined that the plaintiff was likely to prevail under both of the anti-trafficking provisions of the DMCA, and issued an injunction.[54]

In *Universal Studios, Inc. v. Corley*,[55] a group of eight motion picture studios sought to enjoin Internet web site owners from posting a computer program known as DeCSS.[56] This program circumvented CSS, which is the encryption system that protects access to the content on digital versatile disks (DVDs).[57] The Second Circuit upheld an injunction based on the finding that the distribution of DeCSS violated § 1201(a)(2)(A) of the DMCA.[58]

United States v. Elcom Ltd.[59] represents the first criminal case brought under the DMCA.[60] The defendant company marketed software that removed copying and distribution restrictions from digitally formatted books, or "ebooks."[61] The government contended that the marketing of such software violated the § 1201(b) anti-trafficking provision.[62] Although many saw this as a prime example of the type of case for which the DMCA was enacted, the jury ultimately acquitted the defendant.[63]

All of these cases have the common feature of protecting content industry products—video games, music files, videos, and books are all goods whose value lies in the copyrighted content they contain. In contrast, *Lexmark* and *Chamberlain* involve durable goods—products whose value is independent of any ancillary copyrighted software. The background provided in

---

[53] *Id.* at *4.
[54] *Id.* at *12.
[55] 273 F.3d 429 (2d Cir. 2001)
[56] *Id.* at 435-36.
[57] *Id.* at 436-38. CSS is short for "Content Scramble System." *Id.* at 436.
[58] *Id.* at 460.
[59] 203 F. Supp. 2d 1111 (N.D. Cal. 2002).
[60] Criminal liability attaches under the DMCA for willful violations of the anti-circumvention provisions done "for the purpose[] of commercial advantage or private financial gain." 17 U.S.C. § 1204(a)(1)-(2) (2000).
[61] 203 F. Supp. 2d 1111, 1118-19 (N.D. Cal. 2002).
[62] *Id.* at 1119.
[63] *See* Lisa M. Bowman, *ElcomSoft Verdict: Not Guilty*, Dec. 17, 2003, *available at* http://news.com.com/2100-1023-978176.html ("Some lawyers speculated that the jury might have been rendering an opinion on the law itself, as well as on the strict legality of ElcomSoft's activities.").

the next section demonstrates why manufacturers are using the DMCA in this latter, and likely unintended, context.

D. Durable Goods Aftermarkets

Durable goods are products that "yield a flow of services into the future" or that "can be used over and over again," such as washing machines, automobiles, laser printers, or garage door openers.[64] The goods or services supplied for a durable good after its initial sale, such as replacement parts or repair visits, constitute the aftermarket for that product.[65] Durable goods manufacturers thus focus on the full lifecycle of a product when determining its pricing and profitability, evaluating both the initial and aftermarket sales.[66]

Many durable goods manufacturers depend on the aftermarkets of their products to turn a profit, and are thus highly protective of them.[67] These manufacturers sell primary products at or below cost in order to attract customers, then inflate the prices of aftermarket goods or services in order to make their primary sales profitable.[68] For example, a manufacturer may include a free laser printer with the purchase of a new computer, but sell replacement toner cartridges at a significant markup. When the aftermarket costs imposed on consumers are less than the "switching costs" required for consumers to transfer to a different primary product, the consumer is "locked in" to both the original durable good and its aftermarket.[69] Such lock-in pricing strategies fail if aftermarket competitors drive down prices and capture a significant market

---

[64] *See* Michael S. Jacobs, *Market Power Through Imperfect Information: The Staggering of Eastman Kodak Co. v. Image Technical Services and a Modest proposal for Limiting Them*, 52 MD. L. REV. 336, 364 (1993).
[65] *See* Carl Shapiro, *Aftermarkets and Consumer Welfare: Making Sense of* Kodak, 63 ANTITRUST L.J. 483, 485-86 (1995).
[66] *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 118-21 (1999).
[67] *See id.* at 118-19.
[68] *See* Legal Battle Could Determine Future Price of Printer Cartridges, USA Today, Jan. 29, 2003, *at* http://www.usatoday.com/tech/news/techplicy/2003-01-29-printer-battle_x.htm.
[69] *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 103-04 (1999).

share.[70] As a result, primary goods manufacturers seek to exclude aftermarket rivals, sometimes in violation of antitrust laws.[71]

Where primary goods manufacturers have intellectual property rights in aftermarket products, they may legally exercise their right to exclude in order to curtail aftermarket competition. For example, patent holders have the right to prevent others from making, using, or offering to sell their patented products.[72] Manufacturers of computer printers repeatedly exert this right in an effort to prevent third parties from remanufacturing, refurbishing, refilling, or reselling their patented ink cartridges.[73]

II. CASES EXTENDING THE REACH OF THE DMCA

Perhaps because of their experience in enforcing intellectual property rights in the aftermarket setting, printer manufacturers were quick to see the DMCA's paracopyright as a new means for controlling the printer aftermarket. However, unlike enforcing patent rights that inhere in an ink or toner cartridge itself, a manufacturer who invokes the DMCA against aftermarket rivals leverages the paracopyright over uncopyrightable products. The manufacturer shelters its functional products in a fortress of copyrighted software protected by technological measures, a breach of which constitutes a violation of the DMCA. Although a printer manufacturer has successfully used this technique, a garage door opener manufacturer's attempt failed. The legitimacy of this extension of the DMCA is thus still in question.

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

1. Background

[70] *Id.*
[71] *See, e.g.*, Eastman Kodak Co. v. Image Technical Servs., Inc., 504 U.S. 451.
[72] 35 U.S.C. § 271 (2000).
[73] *See* Hewlett-Packard Co. v. Repeat-O-Type Stencil Mfg. Corp., 123 F.3d 1445 (Fed. Cir. 1997).

The plaintiff company, Lexmark International, Inc. ("Lexmark"), is a major competitor in the laser printer industry.[74] In 1997, Lexmark instituted a new marketing strategy known as the Prebate program whereby consumers could obtain an up-front rebate on laser printer toner cartridges through a shrinkwrap agreement that required consumers to return used cartridges to Lexmark for remanufacturing.[75] In order to ensure consumer compliance with the terms of this agreement, Lexmark began installing microchips on Prebate cartridges that would cause printers to malfunction when the cartridges were refurbished by someone other than Lexmark.[76]

In early 2001, Lexmark introduced a new line of microchips for Prebate cartridges used in its T520/522 and T620/622 printers.[77] Lexmark programmed these chips with copyrighted software known as the Toner Loading Program, which monitored the amount of toner remaining in a cartridge.[78] The printers themselves contained copyrighted software known as the Printer Engine Program, which controlled various printer operations, such as paper movement and motor control.[79] The functioning of either program first required the successful completion of an authentication sequence between the microchip on a toner cartridge and the printer.[80]

---

[74] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943, 946 (E.D. Ky. 2003) [hereinafter *Lexmark*].

[75] *Id.* at 947-48. The shirnkwrap agreement that Lexmark placed on each Prebate cartridge box read:

> RETURN EMPTY CARTRIDGE TO LEXMARK FOR REMANUFACTURING AND RECYCLING. Please read before opening. Opening this package or using the patented cartridge inside confirms your acceptance of the following license/agreement. This all-new cartridge is sold at a special price subject to a restriction that it may be used only once. Following this initial use, you agree to return the empty cartridge to Lexmark for remanufacturing and recycling. If you don't accept these terms, return the unopened package to your point of purchase. A regular price cartridge without these terms is available.

Id. at 947 n1.

[76] *Lexmark* Opposition Memorandum, No. 02-571-KSF, at 2.

[77] *See Lexmark*, 253 F. Supp. 2d at 946; *Lexmark* Opposition Memorandum, No. 02-571-KSF, at 2.

[78] *Lexmark*, 253 F. Supp. 2d at 949.

[79] *Id.* at 948.

[80] *Id.* at 952.

The defendant, Static Control Components, Inc. ("SCC"), manufactures, among other items, component parts for refurbished toner cartridges.[81] By October of 2002, SCC had developed the Smartek microchip for use with remanufactured Prebate cartridges.[82] This microchip mimicked the authentication sequence to allow interoperability between Lexmark printers and Prebate cartridges refurbished by unauthorized parties.[83] Although SCC had independently reverse engineered a means for bypassing the authentication sequence, it programmed wholesale copies of the Toner Loading Program onto its Smartek chips.[84]

On December 30, 2002, Lexmark brought suit and moved for a preliminary injunction against SCC.[85] Lexmark claimed that SCC's Smartek chips infringed its copyright in the Toner Loading Programs, and that distribution of the chips violated the § 1201(a)(2) anti-trafficking provision of the DMCA.[86]

2. Analysis

The district court first concluded that Lexmark's claim of copyright infringement was likely to prevail on the merits.[87] SCC admitted that it had made wholesale copies of the program onto its Smartek chips,[88] but raised several defenses for this copying. The court rejected SCC's arguments that the Toner Loading Program was either a lock-out code or a mere constant and formula, or that the copying was protected by fair use. The court also found SCC's copyright misuse argument untenable: SCC asserted that Lexmark's use of its copyrighted programs to secure an exclusive right in the aftermarket for durable goods not expressly granted by copyright

[81] *Id.* at 946.
[82] *Lexmark* Opposition Memorandum, No. 02-571-KSF, at 4.
[83] *Lexmark*, 253 F. Supp. 2d at 955.
[84] *Id.* This crucial fact is still in dispute. *See* Memorandum: Recommendation of the Register of Copyrights in RM 2002-4; Rulemeaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Oct. 27, 2003, at 176.
[85] *Lexmark*, 253 F. Supp. 2d at 947.
[86] *Id.*
[87] *Id.* at 957.
[88] *Id.* at 955.

law constituted misuse, but the court held that copyright law *does* provide for such rights under the DMCA.

The court then determined that Lexmark's claims under the DMCA were also likely to prevail on the merits. The court began its interpretation of the Act by stating that the plain meaning of the statutory language is clear and therefore any appeal to legislative history would be inappropriate. After quoting the § 1201(a)(2) anti-trafficking provision and its accompanying definitions provided in § 1201(a)(3)(A)-(B), the court noted that the term "access" is nowhere defined in the statute and thus the customary, dictionary meaning of the term would apply, namely, the "ability to enter, to obtain, or to make use of."

Thus interpreting the statute in a strictly textual manner, the court concluded that the Smartek microchips violated each of the three alternative tests for liability under § 1201(a)(2) with respect to both the Toner Loading and Printer Engine Programs. The court determined that the authentication sequence constituted a "'technological measure' that 'controls access' to a copyrighted work." Indeed, the sequence controls "access" to two different copyrighted works because a proper authentication sequence is necessary for a printer owner to "make use of" both the Toner Loading and Printer Engine Programs. The court emphasized that Lexmark, the copyright owner of the programs, did not authorize access to its programs. Thus the Smartek chips violated § 1201(a)(2)(1)-(3) because (1) SCC specifically developed the chips to circumvent, (2) the chips had no commercial purpose other than to circumvent, and (3) SCC marketed the chips for their ability to circumvent Lexmark's authentication sequence.

Turning to SCC's defenses, the court again remarked that the clarity of the language of the DMCA prevented any consideration of the congressional intent behind the Act. The court rejected SCC's assertion that the drafters of the DMCA were only concerned with preventing

digital piracy, and thus had not intended such an expansive application of the statute. According to the court, the § 1201(b) ban on tools used to circumvent use controls is sufficient to prevent digital piracy, thus SCC's restricted reading of the DMCA would render the ban on tools used for access in § 1201(a)(2) "mere surplusage." The court further stated that, as drafted, the DMCA is not limited to copyrighted works that have independent market value, such as books, CDs, and motion pictures. Rather, any work entitled to protection under the Copyright Act is also entitled to the DMCA's anti-circumvention provisions.

The court concluded that the reverse engineering exception under § 1201(f) did not apply to the Smartek microchips because they contained verbatim copies of the Toner Loading Program. Section 1201(f) permits the marketing of access-circumventing devices "solely for the purpose of enabling interoperability of an independently created computer program with other programs." Although the Smartek chips contained independently created software that mimicked the authentication sequence, the Toner Loading Program itself was copied, and therefore was not "independently created."

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

1. Background

The plaintiff, Chamberlain Group, Inc. ("Chamberlain"), is the leading manufacturer of garage door openers (GDOs) in the U.S. GDOs typically consist of a garage-based receiver and a transmitter that emits a signal of a fixed digital code to activate the system. Chamberlain developed a new "Security+" line of GDOs that continually alters the activation code—a system known as "rolling code." According to Chamberlain, this system prevents burglars from recording transmitted signals for later retransmission and unauthorized garage access. Copyrighted software within the transmitter encodes the transmitted signal with both a fixed

identification number and a variable number that changes by a factor of three with each use. Copyrighted software within the receiver determines whether the variable portion of a signal falls within an acceptable forward range of values, or "forward window," and if so, instructs a microprocessor to operate the garage door. If the signal falls within the "rear window" of previously-used values, the software will not operate the door.

Chamberlain included a failsafe measure in its software to ensure that the GDO would operate even if a user inadvertently pressed the transmitter button enough times to advance the rolling code past the upper range of the forward window. This process, called "resynchronization," requires the user to depress the button a second time after a failed first attempt. The receiver software compares the two values received in sequence, and operates the GDO if the variable values are separated by a factor of three.

The defendant, Skylink Technologies, Inc. ("Skylink"), markets and distributes GDO components. Skylink sold a universal transmitter capable of operating many different GDOs, including Chamberlain's Security+ line. Consumers who purchased this transmitter Rather than using rolling code software in its transmitter, Skylink exploited the resynchronization process to operate Chamberlain's GDOs. Chamberlain claimed that by circumventing the rolling code technology, thereby gaining access to the copyrighted software in the receivers that operated the GDOs, Skylink's universal transmitters violated § 1201(a)(2) of the DMCA. The court denied Chamberlain's motion for summary judgment on its DMCA claim on August 29, 2003, but invited Skylink to file for summary judgment. The court granted Skylink's motion on November 13, 2003.

2. Analysis

In the August 29th opinion, the court concluded that disputes over several issues of material fact prevented it from granting the plaintiff's summary judgment motion. The first issue was whether Skylink's universal remote was designed and marketed *primarily* to circumvent Chamberlain's protection measure to gain access to the software in the receiver which operated the garage door, given that it could also operate other garage door openers. The court found it unnecessary to fully address this issue since the motion could be defeated on other grounds.

The second issue was whether the computer program in Chamberlain's rolling code was in fact a work protected by copyright. Because this essential element for a prima facie case under section 1201(a)(2) was in dispute, the court denied summary judgment.

Finally, the court addressed the issue of whether a consumer's use of the Skylink transmitter was an "authorized" act for purposes of the DMCA—a separate requirement in the prima facie case that could also independently defeat a summary judgment motion. The DMCA defines circumvention as an act "without the authority of the copyright owner." The court concluded that Chamberlain gave its authority to consumers to use any replacement transmitter they desired. This authority was implicit, and was based on the facts that (1) Chamberlain did not restrict consumers' aftermarket options by shrinkwrap agreement and (2) a history in the GDO industry of universal transmitters indicated an implied license. Essentially, by not explicitly denying its consumers permission to access its copyrighted software, Chamberlain implicitly gave them authority for purposes of the DMCA.

In the context of the authority issue, the court also noted that consumers had a reasonable expectation to access their garages if they were to lose an original transmitter. The court noted that under Chamberlain's interpretation of the DMCA, a homeowner would violate the Act by accessing her garage via her GDO if she had lost her transmitter but had found some other way

to bypass the access system to the copyrighted software. According to the court, "the DMCA does not require such a conclusion."

In granting Skylink's motion for summary judgment, the court focused solely on the fact that Chamberlain had failed to prove that its customers did not have authority to access the copyrighted software in the Security+ GDO receivers. The court used the same reasoning it had in its first opinion. Chamberlain argued that even if consumers had authority to access the software, sellers of replacement transmitters did not. The court rejected this argument by appealing to its analysis in the first opinion. The court stated that

> (1) there is a history in the GDO industry of marketing and selling universal transmitters; (2) Chamberlain has not placed any restrictions on the use of competing transmitters to access its Security+ GDOs; and (3) in order for the Skylink transmitter to activate the Chamberlain garage door, the homeowner herself must choose to store Skylink's transmitter signal into the Chamberlain GDO's memory."

III. DISCUSSION

Application of the DMCA to durable goods aftermarkets raises concerns for the aftermarket industry as a whole.[89] For example, the Automotive Aftermarket Industry Association fears that the *Lexmark* decision could prompt automobile manufacturers to install inexpensive microchips programmed with copyrighted software that would lock out unauthorized brake shoes, air filters, or other replacement parts, thereby jeopardizing the multi-billion dollar independent automotive aftermarket industry.[90] Based on *Chamberlain*, such a

[89] *See* James E. Guyette, *Aftermarkets Urged to Challenge 'Intellectual Property' Ruling*, Oct. 14, 2003, AFTERMARKET BUSINESS.
[90] *See* Motion of Automotive Aftermarket Industry Association, Lexmark International, Inc. v. Static Control Components, Inc. at 2.

marketing strategy may be legally enforceable insofar as the manufacturers employ shrinkwrap agreements that notify customers that authorized replacement parts are the only ones permitted. A reexamination of the DMCA itself, as well as the possible availability of the equitable doctrine of misuse in the anti-circumvention regime, suggest that such fears may not be warranted.

A. Legislative Intent

Although the *Lexmark* court properly started its analysis of the DMCA anti-circumvention provisions with the text of the statute itself, it is evident from the legislative history of the Act that Congress did not intend for the result that was reached, or at the very least did not consider the consequences of its language.[91] Perhaps, then, a form of statutory interpretation other than textualism should be used for the anti-circumvention provisions.

Textualism is a limited strategy for statutory interpretation.[92] Language that appears clear on its face may actually be more nuanced when cast in the light of legislative history. Thus, while the *Lexmark* court repeatedly referred to the statutory language as "unambiguous" and "clear," many copyright scholars who closely followed the protracted development and adoption of the provisions find the exact opposite to be true. For example, Pamela Samuelson stated that "the anti-device provisions of the DMCA are *highly ambiguous* and overbroad,"[93] and David Nimmer suggested that the DMCA "require[s] its vast apparatus of historical material simply in order to be comprehensible."[94] Such statements seem to justify an appeal to the legislative history to determine whether Congress intended the DMCA to apply to durable goods aftermakets.

---

[91] *See* Burk, *supra* note 6, at 1109.
[92] *See* William N. Eskridge, Jr. & Philip P. Frickey, *Statutory Interpretation as Practical Reasoning*, 42 STAN. L. REV. 321, 340-45 (1990).
[93] Samuelson, *supra* note 21, at 524. *See also* David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909, 964 (2002) ("[W]ithout the context that legislative history furnishes, the already impenetrable language of the Digital Millennium Copyright Act would become utterly unfathomable.").
[94] *See* Nimmer, *supra* note 93, at 965.

An examination of the DMCA's legislative history reveals Congress' primary purpose in enacting the anti-circumvention provisions: to curtail piracy of intellectual property while preserving legitimate competition. This is clear both from the language of the WIPO Treaties—from which the DMCA directly followed—and from the legislative history of the Act itself. Congress explicitly stated that the purpose of the DMCA was "to make digital networks safe places to disseminate and exploit copyrighted materials." In the hundreds of pages of legislative history, this objective is repeatedly mentioned; clearly, the purpose of the DMCA was to prevent digital piracy of copyrighted materials.[95] Consistent with this purpose, the anti-tracking provisions were "drafted carefully to target 'black boxes' and to ensure that legitimate multipurpose devices can continue to be made or sold…. This provision is designed to protect copyright owners, and simultaneously allow the development of technology."

By adopting several highly specific exceptions to the general rule against circumvention of access and use controls, Congress created a presumption that any act of circumvention not enumerated in the Act violates § 1201. The highly specific nature of these exceptions makes it hard to interpret the list as merely illustrative, rather than exhaustive. For this reason, Pamela Samuelson has argued that Congress should have included a general purpose 'or other legitimate reasons' exception because the current list does not cover the full spectrum of legitimate reasons for bypassing access controls. Somewhat counterintuitively, it might also have been more desirable for Congress to ban circumvention across the board, thereby allowing courts to use equitable principles to carve out exceptions for legitimate purposes. This is, of course, how the fair use doctrine in copyright law first developed; only later did Congress codify it at 17 U.S.C. § 107.

[95] *See, e.g.*, S. REP. NO. 105-190, at 2 (1998) ("Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy.").

Despite these obstacles in statutory interpretation, courts could still reach a different conclusion than the *Lexmark* court by taking a more purposive approach to the statute. The *Chamberlain* court seemed to start down this road by analyzing factors irrelevant to a DMCA analysis—the legitimate expectation of consumers is nowhere listed in the Act. As did the *Chamberlain* court, other courts can refuse to extend the DMCA to durable goods aftermarkets by applying the statutory canon that "where a statute's plain meaning produces an absurd…result, it is entirely appropriate to consult all public materials, including the background and the legislative history of its adoption."

B. Misuse

Even if courts are bound by the plain meaning of the DMCA, they may still be able to limit the extension of the DMCA into durable goods aftermarkets by using the equitable principle of misuse. Both *Lexmark* and *Chamberlain* courts focused on the license agreements, or lack thereof, between manufacturers and consumers. The *Chamberlain* case may have been decided differently if a shrinkwrap agreement had accompanied the Security+ GDOs. Courts have grappled with the issue of whether such shrinkwrap agreements are lawful in the context of copyright law generally,[96] but this issue may be more nuanced in the context of the new anti-circumvention provisions. Contract provisions often raise the question of misuse.

As seen in *Lexmark*, the copyright misuse defense is unlikely to prevail in DMCA cases. It is for this reason a legal scholar has proposed that the equitable misuse defense be extended to the anti-circumvention provisions. Misuse applies where the ends to which a right, such as paracopyright, is put exceeds the reasonable grant of the right. Based on the prior evaluation of the legislative intent behind the DMCA, it is apparent that the anti-circumvention measures were intended to protect independently marketable copyrighted works. Extending the anti-

[96] *See, e.g.*, ProCD.

circumvention measures into the realm of durable goods, where the copyrighted software is only ancillary to a product's desirability, can therefore be classified as a misuse. Thus, creating contracts that restrict the types of toner cartridges or GDO transmitters a consumer may use may be improper leveraging of the paracopyright right.

B. Statutory and Librarian of Congress Exceptions

Congress anticipated that certain acts of circumvention not enumerated in the statute would be permissible, and thus provided for rulemaking proceedings. However, any exception adopted by the Librarian of Congress would be insufficient to protect activities such as SCC's or Skylink's since the exceptions only apply to § 1201(a)(1). Even if a certain use is exempt from liability under § 1201(a)(1), a manufacturer would still be precluded from trafficking in a device that falls under the exemption.

Nevertheless, SCC proposed three new exemptions during the last round of rulemaking proceedings. The most general of these exemptions was for "[c]omputer programs embedded in a machine or product and that control the operation of a machine or product connected thereto, but that do not otherwise control the performance, display or reproduction of copyrighted works that have an independent economic significance." This exemption touches on the most apparent difference between the works Congress intended to protect under the DMCA and the durable goods in *Lexmark* and *Chamberlain*, namely, that the copyrighted programs used in durable goods are not independently marketable. As the *Lexmark* court noted, the statutory language does not make a distinction based on independent marketability, and thus a literal application of the statute applies to all copyrighted works.

The Copyright Office concluded that no exception was necessary for these forms of copyrighted works. Interoperability of aftermarket goods with primary goods can be achieved

through § 1201(f), so long as aftermarket manufacturers do not engage in copyright infringement. Furthermore, § 1201(f) permits the trafficking of the aftermarket devices. Thus the DMCA already contains a provision that limits an expansive application of this Act.

IV. Conclusion

Congress adopted the DMCA anti-circumvention provisions with the intent of defending copyright industries from digital piracy. Initial cases brought under the DMCA fit into this rubric well. Recognizing in the provisions the potential to exclude competition in the aftermarket, primary goods manufacturers took the DMCA on the offensive. Such application of the DMCA should not be allowed. If courts appeal to legislative history, such activity should be circumscribed. Furthermore, the statute itself and the equitable doctrine of misuse serve to curtail such uses of the DMCA.