Don't Circumvent My Dongle! Misinterpretation of the Digital Millennium Copyright Act Threatens Digital Security Technology

Noah J Wald
DON’T CIRCUMVENT MY DONGLE!
MISINTERPRETATION OF THE DIGITAL
MILLENNIUM COPYRIGHT ACT
THREATENS DIGITAL SECURITY
TECHNOLOGY

“Once a new technology rolls over you, if you’re not part of the steamroller, you’re part of the road.”

INTRODUCTION

Imagine a software developer working on a music production program named “SoundWaves” in his computer lab. SoundWaves stands to be a revolutionary program that will enable users to complete tasks once thought impossible using current audio production software programs. Because SoundWaves is an innovative technology, it has the potential to yield substantial profits. To protect SoundWaves until the software developer is ready to market and offer it for sale, he installs a standard alarm security system at his computer lab, preventing unauthorized persons from entering and stealing his program. Suppose Burglar A were to disable or bypass that alarm system, and then Burglar B later came along, entered the lab, and stole SoundWaves. Burglar B would clearly be in violation of the law despite the fact that Burglar A and not Burglar B disabled the security system.

Now apply the same hypothetical to the digital environment. Well aware of the effect of widespread Internet piracy on the music industry, once SoundWaves is fully developed, the software developer lawfully installs a digital security system around the program to prevent theft by Internet piracy, mimicking a customary

2. See, e.g., Cal. Penal Code §459 (2010) (“Every person who enters any house, room, apartment, tenement, shop, warehouse, store . . . or other building . . . with intent to commit grand or petit larceny or any felony is guilty of burglary.”).
practice in the music software industry. If User B were to use a pirated version of SoundWaves created by User A that eliminated the digital security system, it logically follows that this would also be in violation of the law. However, according to a recent decision issued by the United States Court of Appeals for the Fifth Circuit, using a program that has previously had its digital security system disabled is not a violation of any law.

This software developer has invested significant resources to develop and protect SoundWaves against Internet piracy by following industry security practices, but now learns it is legal for others to use pirated versions of his program that defeat these customary security measures. What was once a valuable program with the potential to yield substantial profits is now freely exchanged between Internet pirates. As a result, the software developer fails to break even, let alone make any profit from SoundWaves. In turn, the software developer is deterred from developing new programs for fear of the same result.

The Fifth Circuit recently held that use of a pirated software program that’s dongle was previously disabled was not in violation of the Digital Millennium Copyright Act’s (“DMCA”) anti-circumvention provision. A dongle is representative of the digital security system in the latter half of the above hypothetical. A dongle functions like a tangible key to a digital lock, by restricting users from viewing or accessing a program without the requisite hardware key. On its face, the Fifth Circuit’s holding appears contrary to the express language of the DMCA and reflects the difficulty courts experience interpreting and applying the DMCA.

The DMCA contains two principal anti-circumvention provisions, the first governs the act of circumventing a technological measure, and the second governs the manufacturing, distribution, and sale of technologies designed to circumvent technological protection measures. This Note focuses on the first provision, Section

3. See Paul McGuinness, How to Save the Music Business, ROLLING STONE, Sept. 30, 2010, at 43-44 (stating that between 2004 and 2009 music industry revenues fell from $25 billion to $16 billion as a result of the advance of Internet service providers and online piracy); see also BAN PIRACY, http://www.banpiracy.com (last visited Feb. 11, 2011) (estimating that over half of all commercial audio studios use pirated software).
1201(a)(1)(A), which states that no one may circumvent a technological measure that effectively controls access to a protected work.\(^7\)

Congress enacted the DMCA to provide copyright owners who use technological control measures with legal remedies against the circumvention of those measures.\(^8\) Congress intended for the DMCA to address the deficiencies in copyright protection that became prevalent as technology advanced.\(^9\) While the rights and protections afforded by the DMCA were meant to address some of the holes in copyright protection, it is paramount to note that they are completely separate from the rights and protections afforded by copyright law.\(^10\) The practical interpretations of the DMCA by the courts, however, blur the distinct line between copyright protection and the protection bestowed by the DMCA.

This Note discusses how the Fifth Circuit misinterpreted the DMCA and analyzes why the use of pirated software that disables dongle protection should give rise to a violation of the DMCA, focusing on the negative impact this decision will have on the use of dongle technology in the music industry. Additionally, this Note offers several solutions to remedy the confusion surrounding proper application of the anti-circumvention provision of the DMCA.

Part I of this Note analyzes the technology of dongles and their role in the music industry; the construction, effect, and purpose of the DMCA and its anti-circumvention provision; and the Fifth Circuit’s recent interpretation and application of that provision. Part II analyzes how the Fifth Circuit erred in its interpretation and application of the anti-circumvention provision, focusing on the legislative history of the DMCA, the special rulemaking procedure contained within the anti-circumvention provision, and the apparent

---

7. *Id.* § 1201(a)(1)(A).
9. See Jay Dratler Jr & Stephan M. McJohn, *Cyberlaw: Intellectual Property in the Digital Millennium § 1.02 [1] (ALM Properties, Inc. 2009)* (discussing deficiencies in copyright enforcement that were addressed by the DMCA including the Copyright Act’s failure to reflect the change in the locus of copying from substantial businesses to small businesses and individuals’ homes).
10. See Lee A. Hollaar, *Legal Protection of Digital Information 217-18* (2002) (“It is important to understand that although the anticircumvention and rights management provisions of the DMCA are closely related to copyright, in that they apply to works protected by copyright, but they are separate from copyright law (except for being codified in the same title of the United States Code).”).
conflict between the Fifth Circuit’s ruling and a recent regulation issued by the Librarian of Congress. Part III addresses the negative repercussions that will result from the Fifth Circuit’s holding, particularly the impact upon the music production industry. The majority of cases and articles addressing the DMCA revolve around the motion picture and television industry, and this Note seeks to fill a gap by informing readers of how the music industry utilizes technological protection measures and dongles. Lastly, Part IV proposes several solutions to remedy the confusion that results from the current construction of the DMCA.

I. THE TECHNOLOGY OF DONGLES AND APPLICABLE LAW

“The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom.”

Before analyzing the Fifth Circuit’s decision, it is necessary to identify and understand exactly what a dongle is, the technology behind it, the customary use of dongles within a specific industry, and the provisions of the DMCA that govern such technologies.

A. The Dongle Demystified: Dongle Technology and Its Practical Use

A dongle acts like a tangible key to a digital lock. A dongle is a type of access control technological protection measure (TPM) in the form of an external hardware security key that looks like a jump drive and restricts users from viewing or accessing a computer

12. See, e.g., 321 Studios v. Metro Goldwyn Mayer Studios, 307 F. Supp. 2d 1085 (N.D. Cal. 2004) (addressing DVD encryption of motion pictures); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D. N.Y. 2000) (DVD encryption); Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (DVD encryption); Coxcom, Inc. v. Chafee, 536 F.3d 101 (1st Cir. 2008) (addressing the bypassing of cable television filters); DRATLER & McJOHN, supra note 9, § 2.04 (providing the descrambling of a cable television signal as the classic example of the anti-circumvention rule’s application); Reese, supra note 8, at 629 (contrasting between types of control methods using DVDs as an example).
14. See generally What is a Dongle?, supra note 5.
15. Jump drives are also known as flash drives. See generally What is a Jump Drive?, WISEGEEK, http://www.wisegeek.com/what-is-a-jumpdrive.htm (last visited Feb. 11, 2011) (“The JumpDrive or UFD is a small, portable device about the size of a BIC lighter or package of gum. The body is an encased circuit board with a memory chip, with one end featuring an integrated USB connector. This connector can slide into a USB port on nearly any computer, making the JumpDrive ideal for quickly
program. High-end software purchases often include a dongle. Use of the software will require that the dongle plug into the computer, most commonly through a USB port. When the software program activates, it searches for the dongle before fully launching, and if the software does not detect the dongle, the software will not operate. Dongles are a way to prevent piracy of expensive software. Dongles achieve this goal because if one obtains a copy of a program, that program will be useless without an authorized dongle capable of accessing the software. Moreover, dongles are not susceptible to piracy via the Internet because they are tangible pieces of hardware rather than software or lines of code.

TPMs are the content owner’s weapon against online piracy and functions similarly to digital locks utilized by copyright owners to protect their works. TPMs are classified in one of two ways, either controlling “access” or “use.” TPMs that control “access” do just as the name suggests—they control the ability to access a digital file. When an access control TPM is in use, one may possess a digital file, but one cannot make use of that file. Think of a diary sealed with a lock, with the diary as the digital file and the lock as the access control TPM. One might possess the diary in one’s hands, but without the ability to open the lock, the secrets contained within cannot be read. The most common example of an access control measure is password protection. Without the correct password, one cannot access what the password protects.

The classification of TPMs that control “use” fall into this category because their design aims to protect a right afforded by copyright, such as the right to make and distribute copies. Usage transferring data or programs.”).

17. For information on USB see What is USB 2.0?, Wisegeek, http://www.wisegeek.com/what-is-usb-2.0.htm (last visited Feb. 11, 2011) (“Universal Serial Bus (USB) . . . is an external serial interface used on computers and other digital devices to transfer data using a USB cable.”).

18. See MGE, 622 F.3d at 364.

19. See generally What is a Dongle?, supra note 5.

20. Id.


22. See id. at 70 (referring to TPMs that control use as copy control devices).


control TPMs involve technologies that manipulate and control the content that is protected.\textsuperscript{25} Such usage control TPMs may control the timeframe of usage depending on the price paid.\textsuperscript{26} Movies On Demand, available through modern television cable services, are a common example of a usage control TPM.\textsuperscript{27} A usage control TPM can also prevent the copying of the underlying data by restricting the ability to copy the actual file. The usage control TPM manipulates the actual content or protected file; as opposed to an access control TPM, which acts as a digital wall around the protected content or file. As technology advances, content owners are developing merged TPMs that control both access and use.\textsuperscript{28}

With an understanding of access and usage control TPMs, it is possible to classify the dongle as an access control TPM. A dongle is an access control TPM because it only prevents a user’s ability to access the software initially and does not affect the protected content. The dongle is like the ignition key to a car. Before a car can go anywhere, the driver must first insert the correct key into the ignition. Likewise, a user must insert the correct dongle into the computer before the software application will run.

\textbf{B. The Role of Dongles in the Music Industry}

Dongle use in the music industry illustrates how dongles act as access control TPMs. Dongles play a vital role in the music industry. Primarily, audio engineers use dongles in conjunction with the process of audio recording and production. Before one can understand how the music industry uses dongles, it is first necessary to understand the basic music production process.\textsuperscript{29}

\begin{footnotes}
\item[25] Eschenfelder & Agnew, supra note 23.
\item[26] Id.
\item[27] If the reader is not familiar with On Demand movies, a good, albeit strange, analogy for how usage control TPMs operate would be a book that sprouted legs and walked back to the bookstore after a certain period of time or a movie that grew wings and flew back to the electronics superstore after being viewed a specific number of times.
\item[28] For more information on the merger of access control and usage control technological protection measures see generally Reese, supra note 8.
\item[29] In this Section, the author relies on personal academic and professional experiences in the music and recording industries to help illustrate the dongle’s role. The author has a B.S. in Music Business and an A.S. in Recording Arts from Full Sail University. The author is also a Digidesign Certified Operator of Pro Tools Music Production Software and a freelance audio engineer.
\end{footnotes}
Recording music is an art form of its own, and audio engineers function as creative artists. Audio recording is the act of capturing the physical dimensions of sound and then reproducing those dimensions either immediately or from a storage medium (such as magnetic tape or digital hard drives), and thereby returning those dimensions to their physical acoustic state. An audio engineer is a professional trained to record all of the individual instruments and vocals for a song, a process known as “tracking.” Audio engineers also combine all the individual tracks into one final “mix,” which is the finished product released by the artist for sale and played on the radio. The engineer will tweak various aspects of each individual track to create the perfect balance of all the sound sources, a process known as “mixing.” For example, the engineer will adjust the volume (loudness) and the panning (where sound sits in the stereo spectrum, e.g. coming out of the left or right speaker) of each track to make the “mix” sound as pleasing as possible.

Using the Beatles may serve as an example to illustrate the audio engineer’s role in the music production process. If The Beatles were to go into a modern studio to record “I Want to Hold Your Hand,” the audio engineer would likely begin by recording the individual

30. See William Moylan, Understanding and Crafting the Mix: The Art of Recording, at xxii (2d. ed. 2007) (“It is widely recognized that the recording process shapes music. Recording techniques and technologies change the qualities of acoustic sound and impart new sound characteristics. These sound qualities are under the control of an individual that shapes the music recording—the [audio engineer]. . . . [The audio engineer] is a musician of sorts—‘conducting’ by encouraging and ensuring quality performances, ‘performing’ recording, mixing, and processing devices, and ‘composing’ the mix.”).

31. Id. at 3.

32. Id. at 311 (“Tracking is the recording of the individual instruments or voices (sound sources) or small groups of instruments or voices, into a multitrack format (DAW, analog multitrack recorder, etc.). This is done in such a way that the sounds can be mixed, processed, edited, or otherwise altered at some future time, and without altering other sound sources.”).

33. Id. at 319 (“Mixing is where the piece of music begins to emerge and ultimately comes together. The mix creates the piece of music, almost in its final form. Here the individual sound sources that were recorded or synthesized are combined into a two-channel or surround-sound recording that will become the final version of the piece after the mastering process.”); see also Ward v. Rock Against Racism, 491 U.S. 781, 786 n.1 (1989) (explaining the concept of mixing volume as applied to a live concert). The mixing concept is the same basic process for both live production and recording applications, the main difference being the final output—speakers at a concert or a CD track. Compare Moylan, supra note 30, at 319, with Ward, 491 U.S. at 786 n.1 (explaining a similar process for mixing a recording and live performance).

tracks. First Ringo’s drums would be recorded, then Paul’s bass, then John’s guitar, then George’s guitar, and finally the vocals. At this point, the engineer would have at least five individual “tracks.” The engineer would then combine all of these individual tracks into one final “mix” that becomes the iconic classic. The engineer is like a cook making a pot of stew, and the individual instruments or tracks represent the protein, potatoes, celery, and carrots. The engineer will take these “ingredients” (the tracks) and mix them all together to create the final “stew” (the mix).

Traditionally the analogue console functions as the engineer’s tool for mixing tracks, which is the giant piece of equipment with thousands of buttons, lights, and knobs that is seen in almost any television program or motion picture containing a scene of a recording studio. Thanks to the digital revolution, what once required the use of expensive and massive analogue consoles can now be accomplished entirely with computer software. The modern industry standard for music and post-production (sound for film, video, and multimedia) software is a program called “Pro Tools,” created by a company named Digidesign, which is owned by a company named Avid. Pro Tools works as a multi-track software-based digital recording and editing system that provides a digital platform on which engineers create mixes. Essentially, Pro Tools Software acts like a giant analogue console contained within a computer. Pro Tools Software requires a dongle to operate, and Pro Tools named its dongle the “iLok.” The use of an iLok, however, extends past just controlling initial access to the Pro Tools software.

35. THE BEATLES, I WANT TO HOLD YOUR HAND (Capitol Records 1964).
36. See AVID TECHNOLOGY, INC., & FRANK D. COOK, PRO TOOLS 101 OFFICIAL COURSEWARE, VERSION 9.0 xxii (2011) (“Pro Tools—the most widely used application for music and post-production in the world today—is a Digital Audio Workstation (DAW) that uses the power of the personal computer to integrate hard disk audio recording, graphical audio editing, MIDI sequencing, digital signal processing (DSP), and mixing into a fast and intuitive application for personal and professional projects.”).
37. Id. at 4.
38. Id. at xxiii (“Over the years, Pro Tools has emerged as the hub of the mixing process.”).
39. Id. at 31 (“Pro Tools 9 software is protected with an iLok key, as are many other Avid third-party software products and plug-ins. Using an iLok for Pro Tools enables you to use a single key for all of your plug-ins and software options.”); see also iLok Information, DIGIDESIGN, http://archive.digidesign.com/support/ilok (last visited Feb. 11, 2011).
Signal processors represent some of the most commonly used audio tools. The audio engineer uses signal processors to shape and craft sounds to develop the character and quality of those sounds. Modernly, many signal processors are in the form of “plug-ins.” The use of dongles in the music industry is most prevalent with regard to protecting software plug-ins. Plug-ins are software modules that add to the functionality of an application. They are mini programs that operate within another program to increase that program’s ability and power. A plethora of companies develop plug-ins for use in music creation, the majority of which are compatible with Pro Tools. Digidesign and Avid also develop their own plug-ins for use with Pro Tools Software. These plug-ins can be extremely expensive and are often what sets professional recordings or mixes apart from amateur projects. To build off the earlier stew analogy, the plug-ins are like the secret spices and herbs that set that stew apart from the average stew. The engineer uses plug-ins in conjunction with Pro Tools to precisely refine the mix, as well as to add unique and creative aspects.

Recently Digidesign transitioned all authorizations for its plug-ins so that they reside on iLoks. The majority of Pro Tools-
compatible plug-ins also utilize the iLok dongle as a TPM. The iLok dongle system was designed to make plug-ins portable, safe, and convenient. Audio engineers commonly work freelance on individual projects for a variety of clients or as in-house engineers at a single studio. Clients, such as recording artists, book studio time for recording and mixing sessions and either use the in-house engineers at the studio or independently hire audio engineers to suit their individual requirements. Like other types of artists, audio engineers develop their own style and skills and utilize plug-ins that accommodate their personal preferences and requirements. Due to the great expense of high quality plug-ins, not every recording studio will possess each plug-in an engineer may desire.

Digidesign and other audio plug-in developers met this problem with an ingenious solution—by offering their plug-in software for free download on their websites, but requiring a dongle containing a purchased license to operate the software. When purchasing a plug-in, a user is only purchasing the license or authorization for that plug-in. The user will then download and store the license to their iLok (or similar dongle).

This process enables an engineer to contact a studio in advance and request the studio download any plug-ins the studio does not already possess but the engineer wishes to use on a specific project. When the engineer arrives at that studio, he will plug his own personal dongle into the studio’s computer to access and utilize the downloaded plug-ins. Without proper authorizations on the iLok, the plug-ins will not operate. The studio that downloaded the plug-ins at the engineer’s request will be unable to utilize them unless the studio purchases its own licenses and downloads them to the studio’s own dongle. This practice of offering plug-ins as free downloads and restricting access by requiring dongles has created and fostered the current market for audio software plug-ins.

49. See MOYLAN, supra note 30, at 319.
50. See AVID TECHNOLOGY, INC. & COOK, supra note 36, at 31 (“The iLok is a USB smart key that contains licenses for your protected software products. . . . The original iLok design stored more than 100 separate licenses from multiple software vendors on a single key; the new design will store up to 500 separate licenses. The iLok enables you to carry your software licenses with you wherever you go in a portable, convenient, and hassle-free key.”).
The music industry relies heavily on dongle protection. By utilizing dongles, software developers can prevent the unauthorized access of their software and render pirated copies useless. The dongle is the tool selected and employed by software developers in the music industry to prevent digital theft of their products. Without the protection afforded by dongles, not only are software developers more susceptible to Internet piracy and unauthorized use of their programs, but the entire industry’s practice of making plug-ins portable and convenient is at risk of obsoletism.

C. The Digital Millennium Copyright Act

With a basic understanding of the technology of dongles and a working example of how individuals utilize dongles, it is now possible to analyze the laws surrounding these technologies. This Section examines the origins of the Digital Millennium Copyright Act, the individual provisions of the Act, and emphasizes the Act’s distinction from copyright law.

1. The Origin of the DMCA

The Digital Millennium Copyright Act, commonly called the DMCA, is the statute implementing two international treaties: the World Intellectual Property Organization (WIPO) Copyright Treaty\(^ {51} \) and the WIPO Performances and Phonograms Treaty\(^ {52} \). The United States and other participating countries signed these treaties to introduce new international rules and clarify existing rules in order to provide adequate solutions to questions raised by new economic, social, cultural, and technological developments.\(^ {53} \) These treaties recognized the profound impact of the development and convergence of information and communication technologies on the creation and use of literary and artistic works.\(^ {54} \) Additionally, these treaties emphasized the outstanding significance of copyright protection as an incentive for literary and artistic creation.\(^ {55} \)

---

53. WIPO Copyright Treaty, supra note 51, at 68.
54. Id.
55. Id.
The two WIPO Treaties included nearly identical provisions on technological measures of protection, which proved to be the most substantial provisions contained in these treaties. The early forms of anti-circumvention provisions stated:

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

Congress passed the DMCA on October 28, 1998, and some call it the “first real example of ‘cyberspace law.’” Five Titles comprise the DMCA, and this Note focuses on Title 1, which specifically implemented the two WIPO Treaties.

2. The Provisions of the DMCA

The DMCA contains very technical provisions based on complicated technologies. As a result, the DMCA is far from plain language and is more akin to reading the manual for a wireless network router. Thus, it is necessary to translate and analyze the language of the DMCA.

Title 17, Chapter 12 of the United States Code codifies the DMCA and contains three separate rules providing legal reinforcement for technological measures protecting copyrighted works. Simply speaking, these rules outlaw the use and distribution of tools that can bypass TPMs. The first of these rules is stated in Section 1201(a)(1)(A) and serves as the focus of this Note. Section 1201(a)(1)(A) is also known as the “anti-circumvention rule.”

---

57. See Dratler & McJohn, supra note 9, § 2.02.
58. WIPO Copyright Treaty, supra note 51, at 71.
59. Dratler & McJohn, supra note 9, § 1.02.
60. For information on the other Titles of the DMCA see Dratler, supra note 9, § 1.02 n.9; 17 U.S.C. §§1201-1205 (1999).
61. See, e.g., 17 U.S.C. § 1201(a)(1)(A) (“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”); 17 U.S.C. § 1201(b)(1)(A) (“[P]rimarily 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.”).
63. See Hollaar, supra note 10, at 208.
section, titled “Violations regarding circumvention of technological measures,” states “[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title.”

Commentators commonly refer to Section 1201(a)(2) and Section 1201(b)(1) as the “anti-trafficking rules.” Section 1201(a)(2)(A) prohibits the trafficking of products, devices, or technologies that “effectively control access to a work protected under this title,” while Section 1201(b)(1)(A) prohibits the trafficking of products, devices, services, or technologies that “effectively protects a right of a copyright owner under this title . . . ”

These three rules differ both in regard to what they apply to as well as when they apply. The anti-trafficking rules prohibit the marketing, sale, and distribution of products and devices that circumvent technological protection measures designed to control access or to protect rights afforded by copyright (usage control TPMs). The anti-circumvention rule, on the other hand, only prohibits the very act of circumventing access control TPMs. These three rules may be summarized as follows:

- **Section 1201(a)(1) – anti-circumvention of access control measures**
- **Section 1201(a)(2) – anti-trafficking of access control measures**
- **Section 1201(b)(1) – anti-trafficking of usage control measures**

The three rules contained in Section 1201 seek to avoid circumvention and the trafficking of devices that aid in circumvention. Trafficking a device or product is a simple concept to comprehend, but the idea of circumvention requires further inquiry.

---

67. *Id.* § 1201(a)(1)(A).
68. *Id.* § 1201(a)(2).
69. *Id.* § 1201(b)(1).
70. See Dratler & McJohn, *supra* note 9, § 2.03.
72. *Id.* § 1201(b)(1)(A).
73. For a more complete analysis of access control measures vs. copy control measures see Reese, *supra* note 8, at 622.
74. See *id.* at 623.
75. See Dratler & McJohn, *supra* note 9, § 2.03.
and explanation. Section 1201 defines to “circumvent a technological measure” as meaning “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.”  Simply stated, “to circumvent” is the act of slipping around, or sidestepping an existing TPM. It is crucial to realize that the anti-circumvention rule prohibits the very act of circumvention and requires nothing more for a violation. Descrambling a cable television signal represents a classic example of the rule’s application. The TPM controlling access would be the scrambling, and descrambling the signal would be the act of circumventing the TPM.

3. The DMCA as Distinct from Copyright Law

Although located in the same title of the United States Code, the DMCA is separate from the laws of copyright. Confusion may arise because the DMCA applies to works protected under copyright law. Possession of a copyright merely acts as a condition precedent to protection under the DMCA. While the DMCA applies only to works protected by copyright, violations of the DMCA give rise to separate causes of action and remedies that are in no manner dependent upon a valid claim under the laws of copyright.

The DMCA outlines civil remedies and provides criminal offenses and penalties for violations of the DMCA. A person who violates the anti-circumvention or anti-trafficking rules is liable either for actual damages, including profits of the violator, or statutory

77. Id. § 1201(a)(3)(A).
78. See Reese, supra note 8, at 623.
79. DRATLER & McJOHN, supra note 9, § 2.04.
80. Id.
82. The individual rules of the DMCA state that the rules apply to “works protected under this title.” Because the DMCA is located within the same title as the laws of copyright, “works protected under this title” refers to works protected by copyright. See 17 U.S.C. § 1201(a)(1)(A) (“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”) (emphasis added); 17 U.S.C. § 1201(a)(2)(A)-(C) (“to a work protected under this title.”).
83. See, e.g., 17 U.S.C. § 1201(a)(1)(A) (stating that the protection afforded by this section applies “to a work protected under this title.”) Title 17 of the U.S.C. is where the Copyright Act is codified. 17 U.S.C. § 106. Therefore, when the DMCA refers to “a work protected under this title,” it is referring to copyright works.
84. DRATLER & McJOHN, supra note 9, § 2.03.
85. 17 U.S.C. §§ 1203, 1204 (1999) (Section 1203 covers civil remedies; section 1204 covers criminal offenses.).
damages “in the sum of not less than $200 or more than $2,500 per act of circumvention, [or per each instance of trafficking a] device, product, component [used to circumvent a TPM].”\textsuperscript{86} The DMCA empowers courts to grant temporary and permanent injunctions as necessary to prevent or restrain a violation, impound devices or products, and to order the modification or destruction of devices or products involved in the violation.\textsuperscript{87} The DMCA also empowers courts to award reasonable attorney’s fees to the prevailing party in a civil action brought under the DMCA.\textsuperscript{88}

A violation of the DMCA that is committed “willfully and for the purpose of commercial advantage or private financial gain” will give rise to criminal punishment.\textsuperscript{89} The express criminal penalties include monetary fines of not more than $500,000 for the first offense and not more than $1,000,000 for each subsequent offense.\textsuperscript{90} Violations of the DMCA may also lead to imprisonment, not exceeding five years for the first offense and ten years for subsequent offenses.\textsuperscript{91} The independent civil and criminal causes of action contained within the DMCA further illustrate that the DMCA operates separately from the laws of copyright.\textsuperscript{92}

\section*{II. THE FIFTH CIRCUIT’S INTERPRETATION OF THE DMCA}

The Fifth Circuit recently interpreted the DMCA’s application to dongle circumvention in \textit{MGE UPS Systems v. General Electric Co.} as a matter of first impression for the court.\textsuperscript{93} The Fifth Circuit originally decided this case in July 2010 and an opinion was published in the advance sheets of the Federal Reporter, but the court granted a rehearing and the opinion was withdrawn and replaced with a much more concise opinion in September 2010.\textsuperscript{94} The original opinion remains available on Lexis Nexis,\textsuperscript{95} and the analysis it

\textsuperscript{86} Id. § 1203(c)(1), (3)(A).
\textsuperscript{87} Id. § 1203(b)(1)-(2), (6).
\textsuperscript{88} Id. § 1203(b)(5).
\textsuperscript{89} Id. § 1204(a) (Like section 1203, section 1204 also applies to violations of section 1202.).
\textsuperscript{90} Id. § 1204.
\textsuperscript{91} Id. § 1204(a)(1)-(2).
\textsuperscript{92} See supra notes 85-91 and accompanying text.
\textsuperscript{94} Id. at 363.
\textsuperscript{95} MGE UPS Sys. v. Gen. Elec. Co., No. 08-10521, 2010 U.S. App. LEXIS 14891, at *7-9 (text of withdrawn opinion), 612 F.3d 760 (5th Cir. 2010) (noting grant of rehearing and withdrawal of opinion), \textit{reh'g granted, withdrawn, and...}
contains remains worthy of critical evaluation to fully understand the rationale behind the court’s final holding.

In its July 2010 opinion, the Fifth Circuit adopted its rationale from the case *Chamberlain Group v. Skylink Techs.*, a 2004 Federal Circuit case.\(^96\) *Chamberlain* was also a case of first impression for the Federal Circuit.\(^97\) With little other precedent, the Fifth Circuit invested great reliance in the Federal Circuit’s ruling in *Chamberlain*. The issue, however, was as novel to the Federal Circuit as the Fifth Circuit, and the Federal Circuit’s holding in *Chamberlain* contains an error in rationale. The Fifth Circuit searched for precedent to follow, found *Chamberlain*, and applied that holding to the case before it.\(^98\) By adopting the Federal Circuit’s ruling from *Chamberlain*, the Fifth Circuit issued a ruling, which upon deeper review, works contrary to the anti-circumvention provision and the policies of the DMCA. The error in the Fifth Circuit’s rationale ultimately led the court to grant a rehearing and substitute its original opinion with an opinion reaching the same conclusion, but on alternative grounds and with much less detail.\(^99\) This Section analyzes each of these three opinions in turn.

### A. The Federal Circuit’s Application of the DMCA

In *Chamberlain*, the technology at issue involved garage door openers (GDOs).\(^100\) Chamberlain was the manufacturer of a line of GDOs and Skylink was the manufacture of a universal transmitter.\(^101\) Skylink’s universal transmitter was programmable by users to open a variety of GDOs including Chamberlain’s GDOs.\(^102\) Chamberlain’s line of GDOs utilized a copyrighted “rolling code” program that constantly changed the transmitter signal required to trigger the GDO to open.\(^103\) This “rolling code” was a method employed to increase security by preventing burglars from capturing the GDO signal and then using it to open the GDO.\(^104\) Skylink’s universal transmitter,
which did not employ the copyrighted rolling code system developed by Chamberlain, nevertheless allowed users to operate and open Chamberlain’s GDOs that utilized the rolling code. Chamberlain alleged that because its GDOs incorporated computer programs protected by copyright and because its rolling codes are a technological measure that controls access to those programs, Skylink was prima facie liable for violating section 1201(a)(2) of the DMCA. Chamberlain did not allege that Skylink infringed its copyright.

After explaining its first impression interpretation of the DMCA, the Federal Circuit reached the conclusion, later adopted by the Fifth Circuit, that a relationship between access and copy protection must exist before an anti-circumvention violation may be found. The court found Chamberlain failed to prove the “critical nexus” between access and protection, in addition to failing to prove the requisite lack of authorization in order to succeed on its DMCA claim. The court subsequently affirmed the district court’s ruling dismissing Chamberlain’s DMCA claim.

B. The Fifth Circuit’s Original Application of the DMCA

In MGE UPS Systems v. General Electric Co., MGE appealed the district court’s dismissal of its DMCA claim. MGE is a manufacturer of uninterruptible power supplies (UPS), which are machines designed to provide power to crucial operating systems during power outages. The use of some of MGE’s UPS systems required the use of MGE’s copyrighted software programs. This software required a dongle to operate, and if the dongle was not detected when the software launched, the software would not operate properly. Hackers published information on the Internet of how to bypass or “hack” MGE’s software so that it did not require the dongle to operate. Employees of PMI, a company acquired by General

capture transmitter signal because the code would have changed).

105. Id. at 1183.
106. Id. at 1185.
107. Id. at 1197.
108. Id. at 1204.
109. Id.
110. Id.
111. MGE, withdrawn and replaced, supra note 95, at *2.
112. Id.
113. Id.
114. Id. at *2-3.
115. Id. at *3.
Electric (GE) before the suit, obtained at least one copy of the hacked MGE software that did not require use of the MGE dongle.\textsuperscript{116} MGE subsequently brought suit against GE for copyright infringement, misappropriation of trade secrets, unfair competition, conversion, and DMCA violations.\textsuperscript{117} The district court dismissed the DMCA claim, but the jury found that GE misappropriated MGE’s trade secrets, committed infringement, and engaged in unfair business practices.\textsuperscript{118} MGE appealed, inter alia, the dismissal of its DMCA claim and GE appealed, inter alia, the award of damages.\textsuperscript{119}

On appeal, the Fifth Circuit held that “[m]erely bypassing a technological protection measure that restricts a user from viewing or using a work is insufficient to trigger the DMCA’s anti-circumvention provision.”\textsuperscript{120} Essentially, the Fifth Circuit held that bypassing an access control TPM does not give rise to an anti-circumvention violation.

The court stated “[t]he DMCA prohibits only forms of access that would violate or impinge on the protections that the Copyright Act otherwise affords copyright owners.”\textsuperscript{121} The court then reasoned that “[w]ithout showing a link between ‘access’ and ‘protection’ of the copyrighted work, the DMCA’s anti-circumvention provision does not apply.”\textsuperscript{122} When applying these principles to the case at hand, the court determined “MGE ha[d] not shown that bypassing its dongle infringes a right protected by the Copyright Act.”\textsuperscript{123} The court then stated “MGE’s dongle merely prevents initial access to the software . . . . [T]here is no encryption or other form of protection on the software itself to prevent copyright violations.”\textsuperscript{124} This reasoning led the court to conclude “[b]ecause the dongle does not protect against copyright violations, the mere fact that the dongle itself is circumvented does not give rise to a circumvention violation within the meaning of the DMCA.”\textsuperscript{125}

\begin{footnotesize}
\textsuperscript{116} Id.
\textsuperscript{117} Id. at *4.
\textsuperscript{118} Id. at *4-5.
\textsuperscript{119} Id. at *1.
\textsuperscript{120} Id. at *8.
\textsuperscript{121} Id. (citing Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1202 (Fed. Cir. 2004)).
\textsuperscript{122} MGE, withdrawn and replaced, supra note 95, at *9.
\textsuperscript{123} Id. at *10.
\textsuperscript{124} Id. at *9-10.
\textsuperscript{125} Id. at *10.
\end{footnotesize}
The most notable difference between the facts of Chamberlain and MGE is that in Chamberlain, Chamberlain’s customers purchased Chamberlain’s GDOs and were using Skylink’s transmitters to operate them. Therefore, Chamberlain authorized the use of its GDOs. The users owned the GDO system and therefore had the right to use the GDO with whatever transmitter they desired. In contrast, in MGE, GE/PMI was utilizing a copy of pirated software that had bypassed MGE’s dongle protection. MGE did not authorize GE/PMI to use MGE’s software. Instead GE/PMI used a stolen version that eliminated the need to pay for the software and the required maintenance by MGE technicians. The Federal Circuit should have simply found no DMCA violation in Chamberlain because the users of the GDOs were authorized users. There was no need for the Federal Circuit to interpret the DMCA, and the Fifth Circuit should not have applied the Federal Circuit’s interpretation to a set of very distinguishable facts.

C. The Fifth Circuit’s Modified Application of the DMCA

After the Fifth Circuit’s opinion was published in the advance sheets of the Federal Reporter, the court granted rehearing and issued a substituted opinion. In the new opinion, the court eliminated all references to Chamberlain, and also eliminated all discussion of types of access control. The court reduced the entire discussion of the DMCA to only several paragraphs. In this new opinion, the court identified the DMCA issue to be determinative on whether the actions of GE/PMI’s own representatives amounted to circumvention, and not whether MGE’s technological protection measures were circumvented at some point. The court then stated that it, “do[es] not construe ‘bypass’ or ‘avoid’ to encompass use of a copyrighted work subsequent to a circumvention merely because that use would have been subject to a technological measure that would have controlled access to the work, but for that circumvention.”

126. Chamberlain Grp., Inc., 381 F.3d at 1187.
127. Id.
128. MGE, withdrawn and replaced, supra note 95, at *2-3.
129. Id.
131. See id. at 365-66.
132. Id.
133. Id. at 366.
134. Id.
The court found that because MGE did not present any evidence showing that a representative of GE/PMI altered MGE’s software, such that the equipment no longer required a dongle to operate the software and because GE/PMI representatives were only using the software after the alteration occurred, no DMCA violation existed.\textsuperscript{135} Essentially, the court held that no anti-circumvention violation had occurred because GE/PMI used a pirated version of MGE’s software and MGE did not prove that GE/PMI was responsible for creating the pirated version of MGE’s software.\textsuperscript{136}

III. HOW THE FIFTH CIRCUIT ERRED IN ITS INTERPRETATION OF THE DMCA

“Everybody experiences far more than he understands. Yet it is experience, rather than understanding, that influences behavior.”\textsuperscript{137}

The Fifth Circuit’s holding in \textit{MGE}, originally adopted from the Federal Circuit’s holding in \textit{Chamberlain}, demonstrates the difficulties courts experience when interpreting and applying the anti-circumvention provision of the DMCA. The Federal Circuit erred in its interpretation and the Fifth Circuit erred by applying the Federal Circuit’s misinterpretation without analyzing the holding and rationale completely.\textsuperscript{138} The Fifth Circuit had a chance to correct its error in its substituted opinion, but instead merely upheld its criticized ruling on alternative grounds and eliminated any significant or substantive rationale.\textsuperscript{139} Both courts failed to consider the impact their holdings would have on industries that utilize the technology in dispute.

A. Misinterpretation of the DMCA Influenced by Misguided Concerns

A potential conflict with fair use was the main theme in \textit{Chamberlain} and the original \textit{MGE} opinion. By examining the legislative history of the DMCA, as well as a regulation recently issued by the Librarian of Congress, this Section discusses how courts misinterpret the anti-circumvention provision of the DMCA due to

\begin{itemize}
  \item \textsuperscript{135} \textit{Id}.
  \item \textsuperscript{136} \textit{See generally id}.
  \item \textsuperscript{137} \textit{HARRY H. CROSBY \& GEORGE R. BOND, THE McLUHAN EXPLOSION: A CASEBOOK ON MARSHALL McLUHAN AND UNDERSTANDING MEDIA} 54 (American Book Co., 1968).
  \item \textsuperscript{138} \textit{See generally MGE, withdrawn and replaced, supra note 95}.
  \item \textsuperscript{139} \textit{See MGE, 622 F.3d 361, 363}.
\end{itemize}
misplaced concerns of hypothetical conflicts with the doctrine of fair use. This Section first analyzes the flaws in the holdings of Chamberlain and the original MGE opinion and then examines how the substituted MGE opinion remains flawed.

1. Legislative Intent of the DMCA and Concerns of Fair Use

In Chamberlain, the Federal Circuit Court analyzed the statutory structure and legislative history of the DMCA and concluded both “make it clear” that Section 1201 is only applicable to acts of circumvention that are reasonably related to protected rights. The Federal Circuit determined that the most significant and consistent theme running throughout the entire legislative history of the anti-circumvention and anti-trafficking provisions of the DMCA was Congress’s attempt to balance the interests of content creators and content users. When considering this balance, the court emphasized a potential tension between the use of access control measures and “fair use.” The court expressed concerns that an unbalanced result would occur because access control TPMs could possibly prevent the fair use of copyrighted works as well as unauthorized uses. The Fifth Circuit, in MGE, also emphasized the alleged conflict between access control TPMs and potential restrictions on fair use.

Both courts worried that the attempt to balance the interests of content creators and content users would tip in favor of creators if courts permitted content creators to restrict simple “access” and not just the more narrowly defined “access that protected rights afforded by copyright.” Thus, when interpreting the language of the DMCA, the courts determined that Congress did not intend the word “access” to simply mean “access” in its plain language definition. Instead, the courts concluded Congress must have intended for the word “access” to mean, “access that bear[s] a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners.”

141. Id. at 1196.
142. See id. at 1196-99, 1203.
143. See id.
144. MGE, withdrawn and replaced, supra note 95, at *8.
145. See id. at *8-10; Chamberlain Grp., Inc., 381 F.3d at 1202-03.
146. MGE, withdrawn and replaced, supra note 95, at *8; Chamberlain Grp., Inc., 381 F.3d at 1202.
147. MGE, withdrawn and replaced, supra note 95, at *8; Chamberlain Grp.,
A more thorough review of the legislative history of the DMCA reveals the redundancy of these concerns. The Federal Circuit was correct when it acknowledged that a primary concern of Congress was the balance between the rights of content creators and content users, but the Federal and Fifth Circuits failed to recognize that Congress confronted this concern and accommodated it accordingly in the present construction and language of the DMCA.

a. Fair Use: A Moot Point

The courts in *MGE* and *Chamberlain* were fixated on potential restrictions of fair use and interpreted the anti-circumvention provision to accommodate this concern. The Federal and Fifth Circuit’s concern regarding fair use was, however, a moot point. The drafters of the DMCA already resolved this concern by developing a rulemaking procedure to selectively waive the prohibition on circumvention.

Early drafts of the DMCA were met with strong criticism by opponents concerned with a potential conflict with the doctrine of fair use. As a result, the drafters of the DMCA devoted substantial time and resources to analyzing the implications of the broad prohibition of the traditional principles of fair use. To alleviate fair use concerns, the drafters included in the DMCA a fail-safe mechanism that would allow selective waiver of the prohibition against circumvention to prevent the diminution in the availability of a particular category of copyrighted materials to individual users.

Subsections (B) and (C) of the anti-circumvention provision convert the statutory prohibition against the act of circumvention into a regulation by including a rulemaking procedure. Through this rulemaking procedure the Librarian of Congress determines whether the prohibition against circumvention should be waived with regard to specific categories of works based on real marketplace developments that may diminish otherwise lawful access to works, such as fair use. Subsection (B) of the anti-circumvention rule states that the rule shall not apply to users of particular classes of works if such

*In re Motion Picture Association of America,* Inc., 381 F.3d at 1202.

148. *See supra* notes 142, 144 and accompanying text.
151. *Id.*
152. *Id.* at 36.
persons are, or are likely to be, adversely affected in the ability to make noninfringing uses of that particular class of works. Subsection (C) of the anti-circumvention rule empowers the Librarian of Congress to identify the particular classes of works subject to waiver. Subsection (C) also provides factors that the Librarian examines while making this determination. The Librarian publishes, in the form of federal regulations, lists of classes of copyrighted works determined to have an adverse effect on noninfringing uses, and the anti-circumvention rule will not be applicable to those published classes of works.

Through this rulemaking procedure, the drafters of the DMCA directly addressed and accommodated the concerns that the Federal and Fifth Circuits emphasized in their interpretations, yet this went unrecognized by both courts. In fact, neither the Federal nor Fifth Circuit even referenced this rulemaking procedure in their opinions. Had these courts looked beyond the basic sections of the anti-circumvention rule, they would have recognized that their concerns of fair use and of striking a balance between content creators and content users are provided for within the existing plain language of the DMCA.

i. A Preexisting Successful Balance

Looking at the legislative history, it becomes clear that this rulemaking procedure did in fact result in a balance between the interests of content creators and users. Two members of Congress who opposed the initial draft of the DMCA because of the very concerns that the Fifth and Federal Circuits expressed, later rose to support the present construction of the DMCA because they believed Congress achieved a successful balance between users and creators.

The courts in MGE and Chamberlain were trying to balance interests that Congress already successfully balanced. Their interpretations requiring “access” to mean “access that bear[s] a reasonable relationship to the protections that the Copyright Act

156. The Librarian of Congress is to act upon the recommendation of the Register of Copyrights and is to consult with the Assistant Secretary for Communications and Information of the Department of Commerce. Id. § 1201(a)(1)(C).
157. Id. § 1201(a)(1)(C)(i)-(v).
158. Id. § 1201(a)(1)(D).
159. See generally MGE, withdrawn and replaced, supra note 95; Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1195 (Fed. Cir. 2004).
otherwise affords copyright owners” was an unnecessary and misleading interpretation.\textsuperscript{161}

ii. Fair Use Inapplicable

In addition to accounting for concerns of fair use by developing the aforementioned rulemaking procedure, Congress also included a mandate in the DMCA explicitly stating that nothing in the DMCA shall affect fair use.\textsuperscript{162} Considering that the DMCA is not copyright law, this mandate makes sense.\textsuperscript{163} The anti-circumvention rule deals with the act of circumvention, not the subsequent use after circumvention occurs.\textsuperscript{164} Any fair use would occur after the violation of the anti-circumvention provision, hence Congress’s rationale for including the rulemaking procedure in the DMCA; the fair use defense is inapplicable and irrelevant to the anti-circumvention rule. Plainly stated, there is no such thing as a fair use defense to a violation of the DMCA; instead, the DMCA itself includes provisions—the rulemaking procedure—aimed at protecting the interests of users.\textsuperscript{165} Thinking of this fair use argument outside of the digital context helps to illustrate. If one were to break into a library after hours, it would not be a defense to breaking and entering if the motive were to make a fair use of a book inside.

b. The True Legislative Intent of the DMCA

The courts in both \textit{Chamberlain} and \textit{MGE} rejected the plaintiffs’ arguments for a plain language interpretation of the DMCA, mainly for the reasons discussed above.\textsuperscript{166} These courts lost sight of the true legislative intent of the DMCA. Congress enacted the DMCA to adapt the law to make digital networks a safe place to disseminate and exploit copyrighted material.\textsuperscript{167} However, the Fifth Circuit’s holding in \textit{MGE} fails to make the digital environment a safer place because

\textsuperscript{161} MGE, \textit{withdrawn and replaced}, supra note 95, at *8; \textit{Chamberlain Group, Inc.}, 381 F.3d at 1202.
\textsuperscript{162} 17 U.S.C. § 1201(c).
\textsuperscript{163} See \textit{Hollaar}, supra note 10, at 217-18; see also supra Part I (C)(3) (discussing how the DMCA is distinct from Copyright law).
\textsuperscript{164} See \textit{MGE UPS Sys. v. Gen. Elec. Co.}, 622 F.3d 361, 366 (5th Cir. 2010) (“Because § 1201(a)(1) is targeted at circumvention, it does not apply to the use of copyrighted works after the technological measure has been circumvented.” (citing \textit{Universal City Studios, Inc v. Corley}, 273 F.3d 429, 443 (2d Cir. 2001))).
\textsuperscript{165} Nimmer, \textit{supra} note 160, at 723.
\textsuperscript{166} See \textit{Chamberlain Grp., Inc. v. Skylink Techs., Inc.}, 381 F.3d 1178, 1201 (Fed. Cir. 2004); MGE, \textit{withdrawn and replaced}, supra note 95, at *7.
the holding creates a loophole allowing for unpunished piracy of dongle-protected software.

In *MGE*, GE/PMI obtained pirated software so that they could utilize MGE’s software without having to pay for its use.\textsuperscript{168} The Fifth Circuit found this action lawful and consistent with the DMCA.\textsuperscript{169} The Fifth Circuit’s holding implicitly sanctions the use of pirated software that bypasses dongle protection, regardless of whether the use is fair or foul. By creating this loophole and implicitly sanctioning piracy, the Fifth Circuit’s holding neglects the intent of the DMCA to protect MGE’s software in the digital environment. Congress intended for the DMCA to protect content creators like MGE, but the Fifth Circuit refused to afford MGE the protection of the DMCA.

The legislative intent behind the anti-circumvention provision shows that Congress sought to establish a general prohibition against gaining unauthorized access to a work by circumventing a TPM.\textsuperscript{170} To explain this rule, Congress equated the act of circumventing a TPM as the electronic equivalent of breaking into a locked room in order to obtain a copy of a book.\textsuperscript{171} This was the exact analogy Chamberlain used when arguing for a plain language interpretation of the DMCA, but the court rejected this argument.\textsuperscript{172} The Federal Circuit stated that the legislative intent of the DMCA clearly supported its position.\textsuperscript{173} The court, however, rejected an argument taken directly from the legislative history of the DMCA.\textsuperscript{174} This further suggests the flaws in the Federal and Fifth Circuit’s rationale for their interpretations.

2. *The Fifth Circuit’s Error Evinced by Recently Issued Regulation*

Aside from the fair use concerns, the error committed by the Fifth Circuit becomes more profound when compared to a recent regulation issued by the Librarian of Congress.\textsuperscript{175} As part of the rulemaking procedure discussed above,\textsuperscript{176} the Librarian of Congress


\textsuperscript{169} Id. at 366.


\textsuperscript{171} Id. at 17.

\textsuperscript{172} Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1201 (Fed. Cir. 2004).

\textsuperscript{173} Id. at 1202.

\textsuperscript{174} See *Chamberlain Grp., Inc.*, 381 F.3d at 1201.

\textsuperscript{175} 37 C.F.R. § 201.40 (2010).

\textsuperscript{176} See supra Part III (A)(1)(a).
published a regulation, effective on July 27, 2010, establishing new classes of works that are exempt from the prohibition against circumvention.\footnote{37 C.F.R. § 201.40.} One of these exempt classes of works is computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete.\footnote{Id. § 201.40(b)(3).} The rationale behind this exemption is that an authorized user of a program, whose program’s dongle no longer functions properly, should be able to circumvent the dongle to gain access.

The indisputable inference drawn from this exemption is that the circumvention of properly functioning dongles is not exempt from the anti-circumvention rule. If the circumvention of dongles should not give rise to a violation of the anti-circumvention rule as the Fifth Circuit held, the Librarian of Congress would have issued a regulation listing dongles in general as exempt from the rule. The Librarian, though, specifically limited the exemption to dongles that have become obsolete. Although this regulation did not become effective until seven days after the Fifth Circuit’s original holding in \textit{MGE}, this blatant conflict between the Fifth Circuit’s holding and the recent regulation strongly suggests the Fifth Circuit erred.

3. \textit{An Uncorrected Error}

Following the Fifth Circuit’s initial opinion in \textit{MGE}, three amicus curiae briefs were filed in support of rehearing, one on behalf of the Motion picture Association of America,\footnote{Brief for Motion Picture Association of America, Inc. as Amici Curiae Supporting Appellants, \textit{MGE UPS Sys. v. Power Protection Servs.}, 622 F.3d 361 (5th Cir. 2010) (No. 08-10521), 2010 WL 4851678.} one on behalf of the Entertainment Software Association, Business Software Alliance, Recording Industry Association of America, and the Software & Information Industry Association,\footnote{Brief for Entertainment Software Association et al. as Amici Curiae Supporting Appellants, \textit{MGE}, 622 F.3d at 361 (No. 08-10521), 2010 WL 4851679.} and one, most notably, on behalf of the United States.\footnote{Brief for United States as Amici Curiae Supporting Rehearing, \textit{MGE}, 622 F. 3d at 361 (No. 08-10521), 2010 WL 4851680.} In its brief, the United States’ main argument stated that the Fifth Circuit erroneously held that the anti-circumvention provision only prohibits access that would violate the Copyright Act.\footnote{Id. at *4.} The United State’s brief requested the Fifth Circuit eliminate its interpretation of the anti-circumvention provision requiring a link between access and copyright protection, but also
suggested that the court could rely on its alternative holding that MGE failed to meet its burden of proving GE/PMI actually circumvented the dongle.\textsuperscript{183} The United States suggested that the court could affirm it’s holding, but suggested it do so on different grounds.\textsuperscript{184} This was despite making several other arguments as to why the general holding—that did not find an anti-circumvention violation—was in error, including that the holding “essentially render[ed] moot the Librarian of Congress’s authority to adopt, by rule, exemptions to the DMCA’s anti-circumvention provision . . . .”\textsuperscript{185} The United States recognized the glaring flaw in the original \textit{MGE} opinion, but suggested that the court simply rely on an alternative basis for affirming the flawed holding.\textsuperscript{186} The United States suggested that this approach would “preserve and respect the finality of the panel’s decision, while at the same time avoiding the need for en banc or Supreme Court review of the panel’s interpretation of [the anti-circumvention provision].”\textsuperscript{187} This was exactly the course of action the Fifth Circuit chose to take when issuing its new opinion.\textsuperscript{188} However, the Fifth Circuit’s substituted opinion is still in conflict with and contrary to the intent of the DMCA.

In its brief, the United States argued that Congress expressed concern that copyright owners would be unwilling to release digital versions of their works in the online marketplace absent a strong federal prohibition on the circumvention of technological locks.\textsuperscript{189} Here, the Fifth Circuit failed to provide this strong federal prohibition by refusing to hold GE/PMI in violation of the DMCA. As the court pointed out, GE/PMI used a pirated version of MGE’s software, but the court refused to hold GE/PMI in violation because MGE was unable to prove GE/PMI created the original pirated version.\textsuperscript{190} The court ultimately rendered a take-nothing judgment for MGE.\textsuperscript{191}

\begin{footnotes}
\footnotetext[183]{183. \textit{Id.} at *12-13.}
\footnotetext[184]{184. \textit{Id.}}
\footnotetext[185]{185. \textit{Id.} at *7.}
\footnotetext[186]{186. \textit{Id.} at *13.}
\footnotetext[187]{187. \textit{Id.}}
\footnotetext[188]{188. \textit{MGE UPS Sys. v. Gen. Elec. Co.}, 622 F.3d 361, 361-66 (5th Cir. 2010).}
\footnotetext[190]{190. \textit{See MGE}, 622 F.3d at 364, 366.}
\footnotetext[191]{191. \textit{Id.} at 371.}
\end{footnotes}
The court failed to offer any explanation as to how failing to find a party who gains an advantage using pirated software of another party will further the policy of protecting and encouraging distribution of works in the online marketplace. In fact, the court’s holding does just the opposite. By failing to find GE in violation of the anti-circumvention provision, the court is deterring MGE from releasing any future works in the online marketplace. Like the software developer in this Note’s introductory hypothetical, MGE invested a great amount of time and resources to develop its software program, and the court allowed GE/PMI to make use of that program without any form of compensation to MGE.

Furthermore, the court’s holding establishes an almost impossible burden for parties bringing anti-circumvention claims by requiring a party to prove that a defendant was responsible for creating the pirated version instead of just proving that the defendant was using a pirated version. The Internet has provided a worldwide platform for the distribution of digital information and files that make it nearly impossible to track down the origins of a pirated version of software.

The court found that this burden appropriate because the court determined that “bypass” or “avoid” did not encompass use of a work that already had its dongle bypassed. The only rationale offered for this reasoning was that “so broad a construction would extend the DMCA beyond its intended purposes . . . .” Common sense, however, suggests that using a pirated version of a software program that no longer requires use of a dongle is in fact the very definition of “avoiding” and “bypassing” the need for that dongle. Such a narrow construction by the court fails to even minimally fulfill the intended purposes of the DMCA. The Fifth Circuit looked to avoid having its original opinion reversed and thus altered its reasoning to comply with the suggestions of the United States, maintaining the same basic holding, originally derived from flawed reasoning.

B. The Death of the Dongle?

When the Fifth Circuit refused to find GE/PMI in violation of the anti-circumvention provision, the court failed to consider the impact of its ruling on the markets and industries reliant on dongle
protection. One factor the Librarian of Congress must consider when determining whether to waive the anti-circumvention rule for certain classes of works is the effect of circumvention on the market for, or value of, works. Accordingly, the Fifth Circuit should have considered the effect of GE/PMI’s circumvention of MGE’s dongle on the value of MGE’s software, if the court truly was concerned with fulfilling the purposes of the DMCA.

By allowing GE/PMI’s circumvention of MGE’s dongle to go unpunished, the MGE holding opens the door for severe negative impact on the market and value of software protected by dongles. The dongle is the content creator’s tool against piracy, and the Fifth Circuit’s holding may render that tool useless. If other courts adopt MGE’s holding, content creators who rely on dongle protection will face the financial and creative burden of developing new measures to combat software piracy.

By restricting application of the anti-circumvention provision to only the party who initially pirated a software program, the Fifth Circuit puts a nail in the coffin of dongle protection technology. To emphasize and better understand the impact that the Fifth Circuit’s ruling will have on the market and value of dongle-protected works, the impact on the use of dongles within the music industry provides a striking example.

1. The Negative Impact of the Fifth Circuit’s Ruling on the Music Industry

The dongle plays a vital role in the music industry and its use has become increasingly common, but the Fifth Circuit’s ruling stands to eliminate the entire dongle protection process that recently developed and is now customary. The music industry confronted an epidemic of piracy and needed to make its programs more portable and convenient. The industry responded by developing a system that utilizes dongle protection. Developers make their software applications freely downloadable online, but the use of the software remains unauthorized and unavailable without the purchase of a license installed on a dongle. The Fifth Circuit’s holding permitting the circumvention of dongles affords unauthorized users the ability to utilize software that has not been purchased without fear of punishment. Under the Fifth Circuit’s holding, the only remedy

197. See supra Part I(B) (explaining the vital role that dongles play in the music production industry).
software developers have against piracy of their software is to bring infringement suits.\textsuperscript{198} The DMCA was separate and distinct legislation intended to extend the protections customarily enjoyed by content creators via copyright into the digital environment.\textsuperscript{199} If a content creator’s remedy lies only in preexisting copyright violations, then the intent of the DMCA remains unfulfilled.

The Fifth Circuit’s holding also indirectly encourages and facilitates infringement and circumvention. Once a pirated version of a software program becomes available on the Internet, potential users of that software face a choice. Potential users may either pay the often expensive price of the software and receive an authorized dongle, or download the pirated version that does not require a dongle at zero cost. Under the Fifth Circuit’s holding, a user is free to use pirated versions of software, as long as they do not pirate the software themselves.\textsuperscript{200} If use of a program that’s dongle had been disabled were to give rise to a violation of the anti-circumvention rule, the result would be a deterrent effect on the use of pirated versions of software and greater protection for that software in the digital environment, fulfilling the purpose of the DMCA.

The availability of free pirated versions of software and the unpunished use of that software severely diminishes the value of the work. What once existed as a valuable product is now easily obtained for free. The Fifth Circuit’s holding will inevitably eliminate the existing customary industry practice of dongle use, and until the creation of new technologies, software developers will be deterred from making new programs. If software developers continue to have their products disseminated freely over the Internet, it is only a matter of time before developers completely cease spending time and resources researching and developing new software applications. Congress intended the DMCA to extend protections commonly enjoyed by copyright owners into the digital environment, but the Fifth Circuit’s ruling stands to eliminate a customary and accepted form of existing protection.

2. The Current Struggle of Waves Audio

The negative impact on the music production industry resulting from the widespread use of software with disabled dongles is already apparent in the struggles of one music production software developer.

\textsuperscript{198} See generally MGE, 622 F.3d 361.
\textsuperscript{199} See supra Part I(C).
\textsuperscript{200} See supra Part II(C).
Waves Audio is one of the most well known developers of music production plug-ins. Waves Audio plug-ins are considered some of the best available and, as a result, are also some of the most expensive. Waves Audio plug-ins work in conjunction with iLok dongles. Because of widespread piracy of their software that bypasses the iLok dongle, Waves Audio filed numerous lawsuits against those who pirate Waves Audio software. A significant problem facing Waves Audio arises because they must first identify users of their pirated software before individual actions may be filed. In an effort to restrict the piracy of their software, Waves Audio engages in undercover investigations of recording studios to determine if they are using pirated versions of its software. If Waves Audio discovers the use of pirated versions of its software, they will file suit. While this practice is effective against users whom Waves Audio has identified, the widespread reach of the Internet renders this practice ineffective against the large-scale piracy of Waves Audio software.

Waves Audio recognizes the inefficiency of this practice and, in an additional effort to fight piracy, teamed up with an organization called “Ban Piracy.” Ban Piracy is the leading rights advocate for the audio software and digital content industry. Ban Piracy provides global services in intellectual property protection to developers, manufacturers, and distributors of digital audio software. The goals of Ban Piracy are to protect audio software rights, educate the audio software industry, and prosecute...
offenders. According to Ban Piracy, over half of all commercial audio studios use pirated software.

Software developers like Waves Audio and Digidesign should not have to rely on undercover investigations or organizations like Ban Piracy to protect their software against piracy. The DMCA aims to prevent the need for these practices, and Waves Audio represents the quintessential poster child for the kind of content creators Congress intended the DMCA to protect. Unfortunately, the reality is that developers like Waves Audio are not receiving adequate legal protection to help eliminate piracy of their software, and according to the Fifth Circuit, developers like Waves Audio and Digidesign should not be afforded the protections of the DMCA.

IV. ELIMINATING CONFUSION BY AMENDING OR REDRAFTING THE DMCA

The misinterpretation of the DMCA does not rest entirely upon the Fifth Circuit’s shoulders. The language and structure of the DMCA are anything but straightforward to someone unfamiliar with the technology involved. Congress enacted the DMCA in 1998, just as the digital revolution was beginning and new technologies were emerging. The drafters of the DMCA were trying to account for potential problems and issues that could not possibly be imagined at the time of drafting. Thus, it is no surprise that thirteen years later the courts are experiencing difficulty applying the language of the DMCA to recently developed technologies. Congress should redraft the DMCA to update the language to reflect modern technologies, and if Congress redrafted the DMCA, the following suggestions could help add some clarity.

A. Expand the Librarian of Congress’s Power to Issue Regulations

Under the current construction of the anti-circumvention rule, Congress empowered the Librarian of Congress to issue periodical regulations identifying specific classes of works that shall be exempt from the anti-circumvention rule. The Librarian of Congress’s

208. Id.
210. See supra note 59 and accompanying text.
211. See supra note 9 and accompanying text (stating that Congress enacted the DMCA to address the deficiencies in the law as technology evolves).
212. 17 U.S.C. §1201(a)(1)(C)-(D) (1999); see also supra Part III (A)(1)(a) (explaining the rulemaking procedure for selective waiver of the anti-circumvention
power to issue regulations should be expanded to issue regulations identifying specific technologies or actions that trigger the anti-circumvention rule. Under this model, courts would have concrete examples to analogize and differentiate with an individual case’s facts.

Listing everything that would give rise to an anti-circumvention violation may seem burdensome, but if Congress were also to establish factors that had to be met before such technologies or acts were included, the burden would outweigh the benefit. For example, a factor for inclusion could require substantial proof that the circumvention of a specific technology is having a negative effect on the market or value of copyrighted works. The Librarian should also issue inclusive regulations based on trial court decisions finding anti-circumvention violations.

B. Defer All Cases Arising Under the DMCA to a Designated Jurisdiction

Another method Congress should employ to eliminate the confusion surrounding the DMCA and ensure consistent interpretations is to have all cases arising under the DMCA deferred to the Federal Circuit Courts, such as the model employed with patents. Over time, a designated jurisdiction would become more educated and familiar with the DMCA and its application to complex technologies, which would lead to consistent interpretations of the DMCA. Having the Federal Circuit hear all cases arising under the DMCA will provide for consistency and eliminate the need for every circuit court to interpret the DMCA independently, which, as demonstrated by the Fifth Circuit, can lead to error and misapplication.

C. Rename the DMCA and Its Provisions

The DMCA should be renamed in order to more clearly identify the subject matter of its provisions and to distinguish the DMCA from the law of Copyright. While the DMCA presently protects only copyrighted works, its current name and statutory location misleadingly suggest the DMCA is copyright law. This is possibly a current cause of confusion in the interpretation of the DMCA. Renaming the DMCA might create some confusion as to what kinds of works the DMCA applies to, but including a valid copyright as a

---

condition precedent would prevent this confusion. Congress should rename the Act the “Anti-Digital Piracy Act” to better convey the intent and focus of the DMCA. Likewise, Congress should rename the anti-circumvention provision because of the confusing nature and vagueness of that name. Congress should name this provision, “Digital Trespass” to provide a more explanatory and intuitive title than a rule against the circumvention of access control measures.

CONCLUSION

The Fifth Circuit’s interpretation of the DMCA fails to fulfill the intent of the DMCA. The Fifth Circuit originally invested too great an emphasis on concerns of fair use and lost sight of Congress’s principal intent of protecting content creators in the digital environment. The court then elected to preserve the finality of its original holding in place of correcting its error by reaching the same flawed holding on alternative grounds.214 The Fifth Circuit is stripping content creators that utilize dongles of protection in the digital environment, instead of affording more protection where needed.

The Fifth Circuit neglected considerations of the adverse effects of its holding on technologically-dependent industries that currently rely upon dongle protection, like the music production software industry, which relies heavily on dongle protection to combat Internet piracy. The Fifth Circuit has rendered the dongle ineffective in the fight against piracy and indirectly sided with Internet pirates, helping to facilitate circumvention and piracy when the court should be protecting the content creators in the digital environment.

Noah J Wald*

* J.D. Candidate, Thomas Jefferson School of Law, May 2012. B.S. Music Business, A.S. Recording Arts, Full Sail University 2008. Digidesign Certified Operator of Pro Tools Music Production Software. I would like to thank all of my wonderful editors, Paul Cataudella, Sean Vent, Ian Van Leer, Brandon Gray, Flavio Nominati, and Amy Estrada, for all of their invaluable assistance, encouragement and contribution. I would also like to thank Professor Bryan Wildenthal for his critique and contributions. Thank you to my colleague Joe Kinlaw for helping me maintain my sanity throughout this process. Most of all, I would like to thank my parents Karen and Michael for refusing to stop believing in me even when I had.