January 4, 2014

The Evolution of the Digital Millennium Copyright Act; Changing Interpretations of the DMCA and Future Implications for Copyright Holders

Hillary A Henderson, Texas State University

Available at: https://works.bepress.com/hillary_henderson/1/
THE EVOLUTION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT
CHANGING INTERPRETATIONS OF THE DMCA AND FUTURE IMPLICATIONS FOR
DIGITAL COPYRIGHT HOLDERS

December 18, 2013

Hillary A. Henderson – M.A. Legal Studies
TABLE OF CONTENTS

I. OVERVIEW..................................................................................................................3

II. OVERVIEW OF THE DMCA AND THE TENSIONS IT CREATES.........................4

III. TITLE I OF DMCA: ANTI-CIRCUMVENTION .........................................................6

IV. ANTI-CIRCUMVENTION CONTROVERSY .............................................................7

V. TITLE II OF DMCA: SAFE HARBORS .................................................................12

VI. SAFE HARBOR CONTROVERSY ........................................................................16

VII. FUTURE IMPLICATIONS AND POSSIBLE ALTERNATIVES .......................20
I. OVERVIEW

Copyright law rewards an artificial monopoly to individual authors for their creations.\(^1\) This reward is based on the belief that, by granting authors the exclusive right to reproduce their works, they receive an incentive and means to create, which in turn advances the welfare of the general public by “promoting the progress of science and useful arts.”\(^2\)

Copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device . . . . In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.\(^3\)

The Copyright Act of 1976 is the sole federal statute governing copyright law.\(^4\) It was intentionally written in a vague manner and meant to be open to evolving interpretation as technology transforms throughout history.\(^5\) An important (and the most recent) revision of the 1976 act was enacted in 1998, and is known as the Digital Millennium Copyright Act (“DMCA”).\(^6\) Its purpose is to update copyright law for the digital age.\(^7\) The DMCA is the foundation of every United States federal law regarding digital rights.\(^8\)

---

\(^1\) Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975).


\(^5\) Id.


\(^7\) BOUCHOUX, supra note 4, at 187.

\(^8\) Kyle Wagner, Everything Wrong with Digital Copyright (And How to Fix It), GIZMODO (April 21, 2013, 12:02 PM), http://gizmodo.com/5989166/everything-wrong-with-digital-copyright.
Intentional ambiguity enables this law to remain applicable to a variety of modern court cases. However, this same ambiguity also affords courts the freedom to issue widely varying opinions and judgments regarding rapidly advancing technology. To give the reader some perspective of this ambiguity, this article discusses recent judicial applications of the DMCA. Section II outlines the main pillars of the DMCA. Sections III and IV provide more detail about Title I of the DMCA, which deals with anti-circumvention implementation and evolution. Sections V and VI discuss Title II of the DMCA, which addresses safe-harbor protection from the law; this title of the DMCA currently is the most controversial. Section VII pinpoints difficulties that parties governed by the DMCA may face as technology continues to evolve, and section VIII offers alternative ideas that could help bypass some undesirable outcomes.

II. OVERVIEW OF THE DMCA AND THE TENSIONS IT CREATES

On October 28, 1998, President Clinton signed the DMCA into law.\(^9\) It is the most sweeping revision to copyright law in the last thirty years and, according to Tarleton Gillespie, "arguably represents the most dramatic change in the history of U.S. copyright law."\(^{10}\) It passed without much congressional debate, but it was a massive and complex piece of legislation designed to keep United States copyright law in step with constant technological developments.\(^{11}\) Its purpose was to encourage Internet service providers ("ISPs") and copyright owners to cooperate with each other when dealing with copyright infringers.\(^{12}\) It was also designed to

---


\(^{10}\) TARLETON GILLESPIE, WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE 177 (2007).


afford service providers greater certainty concerning their legal exposure for facilitating infringement.\textsuperscript{13}

When considering the DMCA, Congress recognized that the Copyright Act was experiencing difficulty in keeping pace with emerging technology. “The law must adapt in order to make digital networks safe places to disseminate and exploit copyrighted material.”\textsuperscript{14} Additionally, “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 assurances that they will be protected against massive piracy.”\textsuperscript{15}

Two main pillars comprise the DMCA.\textsuperscript{16} Title I, 17 U.S.C. §§1201-1205, affords protection to copyright holders against potential infringers’ circumvention of digital rights management (“DRM”).\textsuperscript{17} Title II, 17 U.S.C. §512, is often referred to as the Online Copyright Infringement Liability Limitation Act (“OCILLA”),\textsuperscript{18} it establishes four safe harbors that protect ISPs from monetary liability for infringing content on their sites posted by third-party users.\textsuperscript{19} The objective of each pillar is noticeably inconsistent with the objective of the other.\textsuperscript{20} Title I expanded copyright liability for potential infringers, while Title II limited liability for this same

\textsuperscript{13} Id.

\textsuperscript{14} Id at 2.

\textsuperscript{15} Id at 8.

\textsuperscript{16} Id.


\textsuperscript{19} Id. § 512(a)-(d).

\textsuperscript{20} Edward Lee, Decoding the DMCA Safe Harbors, 32 COLUM. J.L. & ARTS 233, 233 (2009).
Consumer-rights activists, who would like to see fewer restrictions on copyrighted information, hotly criticize the DMCA. Professionals from the music and movie industries, who advocate for more restrictive legislation, also disagree with the implementation of the DMCA. Kyle Wagner sums up the status of this debate succinctly: “Like umpires in baseball, sometimes if both sides are mad at you, you're doing something right. With the DMCA, that's not entirely untrue, but it's also deeply flawed in certain aspects.” A more detailed discussion of each title and its associated inconsistencies follows.

III. TITLE I OF DMCA: ANTI-CIRCUMVENTION

Title I of the DMCA is based heavily on the international rules established by the Berne Convention. The United States adopted specific anti-circumvention laws for the primary purpose of securing membership in the World Intellectual Property Organization (“WIPO”). The United States desired WIPO membership in order to afford copyrighted works created in the United States the international protections that WIPO established at the Berne Convention. The Berne Convention created laws obligating member nations and states to prevent circumvention of technological measures used to protect copyrighted works, and to prevent

21 Id.

22 Wagner, supra note 8.

23 Id.

24 Id.

tampering with the integrity of copyright management information.\textsuperscript{26} Title I provides legal protection that the international copyright community deems critical to the safe and efficient exploitation of works on digital networks.\textsuperscript{27}

Title I forbids a potential infringer from attempting to subvert digital protection.\textsuperscript{28} Since 1998, when the DMCA was enacted, anti-circumvention protection has grown to encompass a number of different media, namely DRM and phone unlocking.\textsuperscript{29} Originally, Congress intended to introduce specifics into this law as technology evolved, but instead chose to put a system in place that authorizes the Library of Congress to accept applications and grant individual exemptions.\textsuperscript{30}

\section*{IV. ANTI-CIRCUMVENTION CONTROVERSY}

The anti-circumvention title of the DMCA is “one of the most-litigated and controversial provisions of the DMCA.”\textsuperscript{31} It creates significant gray areas regarding liability for DRM circumvention.\textsuperscript{32} Courts have had a difficult time maintaining a balance between the DMCA's

\begin{itemize}
\item[\textsuperscript{27}] \textit{Id.} at 3.
\item[\textsuperscript{28}] \textit{Id.}
\item[\textsuperscript{31}] Mart Kuhn, \textit{Defining “Circumvention”: Another DMCA Case}, PUBLIC KNOWLEDGE (July 23, 2010), http://www.publicknowledge.org/blog/defining-circumvention-another-dmca-case.
\item[\textsuperscript{32}] Pamela Samuelson & Jason Schultz, \textit{Should Copyright Owners Have to Give Notice of Their Use of Technical Protection Measures?}, J. ON TELECOMM. & HIGH TECH. L. 41, 54 (2007).
\end{itemize}
intended purpose of safeguarding digital rights for copyright holders and promoting the free flow of information.33 By using a technical device (DRM) to protect music, images, or words, a copyright holder can turn traditionally permissible use of digital content into a civil violation.34 Examples of activities affected by the provisions of §1201 of the DMCA include: manipulating the computer code of a digital toy to make it perform new functions; disabling an access control device on the storage media of an entertainment product; creating a patch for a software program or electronics product; or performing cryptanalysis on security systems that control access to digital data.35

Approximately one year after the DMCA was enacted, RealNetworks, Inc. became the first Internet entertainment company to file an anti-circumvention suit. The suit was against Streambox.36 RealNetworks offered an online audio and video streaming service. The streaming content could only be played using RealNetworks’ software program.37 Streambox created two software programs capable of disabling the streaming protections of RealNetworks.38 The first of these programs, the Streambox VCR, disabled RealNetworks’ DRM protection and allowed third-party users to download files without restriction.39 The second program, the Streambox Ripper, allowed users to convert these downloaded files to other formats that could be used on

33 DMCA, ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/issues/dmca (last visited Nov. 6, 2010).
35 Id.
38 Id.
39 Id.
other media players.\footnote{Id.}

RealNetworks sued Streambox in the U.S. District Court for the Western District of Washington under the DMCA for circumventing its DRM measures. Streambox claimed a fair-use defense for both the Streambox VCR and the Streambox Ripper because both copyright owners and third-party users could use Streambox to convert their content from RealMedia to other formats; therefore, the Streambox software provided a legitimate function (for the copyright owner).\footnote{Id. at 38.}

The district court found that the Streambox VCR violated two of the three prongs of 17 U.S.C. §1201(a)(2)'s antrafficking provisions: 1) The program is primarily, if not exclusively designed to circumvent RealNetworks’ DRM, and 2) the program’s only commercial purpose was to allow users to access and download protected content.\footnote{RealNetworks, Inc., 2000 WL 127311 at *8.} The court issued a preliminary injunction to stop the distribution of Streambox VCR.\footnote{Id. at 12.}

The district court rejected the fair-use defense of the Streambox VCR by using the “fair use” standard that had been established in Sony Corp. v. Universal City Studios, Inc.\footnote{Sony Corp., 464 U.S. at 417. According to Bruce E. Boyden, Sony created a very influential test for determining the liability of service providers for infringement committed by third-party users. This test asks very simply whether the product or service was capable of substantial noninfringing uses. Previous indirect infringement cases involved dance clubs, hotels, restaurants, and independent contractors. All of these cases were interactions between humans. Sony was the first case in which the courts ruled on a claim that a machine manufacturer should be held liable under copyright law for the way it was used. Bruce E. Boyden, The Most Important Supreme Court Case in Copyright Law: Sony Corp. v. Universal City Studios, MARQUETTE UNIVERSITY LAW SCHOOL FACULTY BLOG, http://law.marquette.edu/facultyblog/2010/11/01/the-most-important-supreme-court-case-in-copyright-law-sony-corp-v-universal-city-studios-1984/ (last accessed October 20, 2013).} Using this standard, the court held that Streambox was entitled to the same protection that the Sony VCRs
had used for their “time-shifting” function. The copyright holders in *Sony* had either authorized or would not object to having their works time-shifted, whereas the copyright holders in *RealNetworks* had specifically chosen to prevent the copying enabled by Streambox. Therefore, Streambox's fair-use defense failed.

The district court did not enjoin the Streambox Ripper, however, because it was found to have legitimate purposes and commercially significant uses, such as allowing copyright owners to convert RealMedia files to other formats. Streambox provided examples to the court of various copyright owners that required a way to convert their own RealMedia files into different formats, such as .WAV for editing, or .WMA to accommodate playback on a Windows Media Player instead of a RealPlayer. In addition, content that was freely available, such as public domain works and material that users were invited and even encouraged to access and copy, could be converted by the Ripper into a different file format for listening at a location other than the original computer.

*RealNetworks* is one of the earliest examples of the confusion courts have had in applying the DMCA’s provisions. A prominent treatise on copyright observes that the enactment of the DMCA meant that the fair-use standard established in *Sony* was no longer a relevant gauge for whether conduct was permitted. At the same time, by allowing the continued use of the second

---

45 *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984). Time-shifting is “the practice of recording a program to view it once at a later time, and then erasing it. Time-shifting enables viewers to see programs they would otherwise miss because they are not at home, are occupied with other tasks, or are viewing a program on another station at the time of a broadcast that they desire to watch.” *Id.* at 423.

46 *Id.* at 417.

47 *RealNetworks*, 2000 WL 127311 at *5.

48 *Id.*

Streambox software, this case also provided the lesson that “it is important to evaluate whether a product that disables copy protections has a legitimate purpose. If so, it is more likely to survive an anti-circumvention attack.”

DMCA inconsistencies are again apparent in a more recent case, *RealNetworks, Inc. v. DVD Copy Control Association.* In this case, RealNetworks was on the other side of the argument, and was enjoined from launching its RealDVD product. The motion picture industry sued RealNetworks over its RealDVD software, which was designed to allow consumers to copy their DVDs to their computers for later playback. On August 11, 2009, the court granted a preliminary injunction in favor of the movie studios and held that RealNetworks had “violated the DMCA's ban on trafficking in circumvention devices by distributing RealDVD products.”

In the mid-1990s, representatives from the movie, electronics, and computer industries came together to form the Copy Protection Technical Working Group. The goal of this group was to develop a standardized technology to prevent the unauthorized duplication of DVD content. The group endorsed the Content Scramble System (CSS), which encrypted the contents of a DVD, rendering it unplayable until it was “unlocked” by CSS “keys” on a DVD drive. The CSS required the presence of the DVD in the drive in order to function.

As a threshold matter in *RealNetworks*, the district court concluded that the CSS was a technological measure that controlled access to protected works and prevented duplication of

50 Nguyen, supra note 37, at 38.


52 Id.

53 Id. at 917.

54 Id.

copyrighted DVD content by the average consumer.\textsuperscript{56} By definition, this qualified the CSS as DRM. The relevant question in \textit{RealNetworks} then became whether the RealDVD product was primarily designed to circumvent the DRM.\textsuperscript{57} The district court concluded that RealDVD was designed primarily for circumvention of the CSS and other protective measures to permit a user to access DVD content without the authority of the copyright owner.\textsuperscript{58}

In contrast, a recent decision issued by the United States Court of Appeals for the Fifth Circuit held that using a computer program that has previously had its digital security system disabled (by a third party) is not a violation of any law.\textsuperscript{59} This decision implies that it is legal for a consumer to use pirated versions of a program.\textsuperscript{60} This, of course, means that a previously valuable program with the potential to yield substantial profits can now be exchanged without reservation between Internet pirates.\textsuperscript{61} As a result, the software developer will no longer be able to recognize a profit from the intellectual property it created.\textsuperscript{62} Ultimately, such a lack of incentive will deter software developers as a group from creating new programs.\textsuperscript{63}

\textbf{V. TITLE II OF DMCA: SAFE HARBORS}

The other major pillar of the DMCA is Title II, which affords safe-harbor protection to

\textsuperscript{56} \textit{Id}.

\textsuperscript{57} \textit{RealNetworks}, 641 F. Supp. 2d at 926.

\textsuperscript{58} \textit{Id}. at 932-35.


\textsuperscript{61} \textit{Id}. at 326.

\textsuperscript{62} \textit{Id}.

\textsuperscript{63} \textit{Id}.
ISPs that host third-party content.\textsuperscript{64} In lay terms, “safe harbor” means that companies such as YouTube and Facebook, which host content uploaded by users, are not responsible for information their users upload.\textsuperscript{65} Without this portion of the law, copyright holders could sue ISPs every time third-party users uploaded any content to their sites.\textsuperscript{66} In theory, a copyright infringement law without safe harbors would bankrupt the entire Internet.\textsuperscript{67} The DMCA safe harbors ensure that the responsibilities of ISPs are limited to removing infringing content without question, immediately, and methodically.\textsuperscript{68} However, not all ISPs are able to qualify for this protection.

The first hurdle that an ISP must clear before it can claim safe-harbor protection is to prove that it meets the threshold requirements of the DMCA. The first of these requirements is that the ISP must meet the definition of “service provider” given by the DMCA.\textsuperscript{69} For an ISP providing information storage, the ISP must be “a provider of online services or network access, or the operator of facilities therefor.”\textsuperscript{70}

Second, an ISP must also accommodate any standard technical measures of digital rights management (“DRM”) that individual copyright owners may choose to employ.\textsuperscript{71} In order to qualify as a standard type of DRM, the technical measure must have been developed by a broad

\textsuperscript{64} Wagner, \textit{supra} note 8.

\textsuperscript{65} Id.

\textsuperscript{66} Id.

\textsuperscript{67} Id.

\textsuperscript{68} Id.

\textsuperscript{69} Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004).

\textsuperscript{70} 17 U.S.C. § 512(k)(1)(B).

\textsuperscript{71} Id. § 512(i)(1)(B).
consensus of copyright owners and ISPs in a fair process, spanning multiple industries; it must be available to any copyright owner on reasonable and nondiscriminatory terms; and it must not impose substantial costs on the ISP or its system.\textsuperscript{72}

Lastly, after validating eligibility and willingness to accommodate reasonable DRM measures, an ISP must adopt, implement, and inform subscribers of a policy that provides for the termination of repeat infringers' accounts.\textsuperscript{73} This threshold requirement is the most stringent, but also the most widely misinterpreted. The legal reasoning behind this requirement is to prevent piracy by encouraging ISPs to cooperate and communicate directly with copyright owners.\textsuperscript{74} If the DMCA did not require ISPs to adopt and enforce a termination policy, especially against repeat infringers, those infringers could effortlessly continue to violate copyrights. For example, once their material was identified and taken down, they could easily re-register (using false information) with the service after being terminated.\textsuperscript{75} Allowing re-registration to happen would render the “realistic threat of losing access” meaningless.\textsuperscript{76}

This strict requirement places a large responsibility on ISPs. However, Congress did not intend this requirement to force ISPs to investigate users for potential infringement, monitor their services, or attempt to catch users who re-register.\textsuperscript{77} The DMCA provides, “Nothing in this section [§ 512 (m)(1)] shall be construed to condition the applicability of [the safe harbors] on a service provider monitoring its service or affirmatively seeking facts indicating infringing


\textsuperscript{73}17 U.S.C. § 512(i)(1)(A).

\textsuperscript{74}A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

\textsuperscript{75}Perfect 10, Inc. v. Cybersnet Ventures, 213 F. Supp. 2d 1146, 1176-77 (C.D. Cal 2002).

\textsuperscript{76}S. Rep. No. 105-190, at 52.

\textsuperscript{77}17 U.S.C. § 512 (m)(1).
activity.”78 Thus, to encourage ISPs to monitor infringement, the information that an ISP finds in voluntary monitoring will not, in theory, be used against the ISP.79

The failure of an ISP to meet these threshold requirements does not necessarily mean that the ISP is liable for copyright infringement. The copyright owner can still demonstrate that the provider has infringed, and the provider can still use other defenses, such as fair use, that are available to copyright holders.80

Once the DMCA threshold requirements are met, an ISP may qualify for safe-harbor protection only if it engages in specific business practices. These practices include transitory communications, system caching, information storage at the direction of users, or information location tools.81 Of these business practices, “information storage at the direction of users” has created the most discord within the entertainment industry.

In order to qualify as an ISP that provides information storage at the direction of users, and therefore for specific safe harbor protection as indicated by 17 U.S.C. §512(c), an ISP must not have knowledge of the infringing activity or facts that make the infringing activity apparent.82 If an ISP is aware of infringing activity, it must “act expeditiously to remove or disable access to the infringing material.”83 Additionally, an ISP cannot receive a financial benefit from the infringing activity if it has the right and ability to control the activity.84

78 Id.


81 17 U.S.C. § 512(a)-(d).

82 Id. § 512(c)(1)(A)(i)-(ii).

83 Id. § 512(c)(1)(A)(iii).

84 Id. § 512(c)(1)(B).
VI. SAFE HARBOR CONTROVERSY

The debate surrounding DMCA safe harbors is multi-faceted. Significant debate has surfaced regarding the validity and general fairness to the copyright holder when an ISP is expected to blindly suppress a copyrighted work immediately, regardless of any future finding of actual liability. This behavior negatively affects the copyright holder by (potentially unfairly) restricting public exposure to the copyrighted work, thus reducing potential for economic gain by the copyright holder. Many critics believe these stringent take-down procedures are contradictory to the First Amendment. Additionally, the courts have yet to rule on exactly how the safe-harbor criteria are to be interpreted, specifically, what constitutes “right and ability to control.”

During the 2008 U.S. presidential race, the John McCain and Sarah Palin campaign reached out to young voters by creating a channel on YouTube, posting video clips and allowing viewers to subscribe to the feed. Weeks before the election, several campaign advertisements were removed from the McCain campaign's YouTube channel and replaced with an advisory: “This video is no longer available due to a copyright claim.” The claimants, including CBS News, Fox News, the Christian Broadcasting Network, and NBC News, alleged that the advertisements had infringed their copyrighted television programs. The McCain campaign responded with a fervent letter to YouTube:

Numerous times during the course of the campaign, our advertisements or web

---

85 Id. § 512(c)(1)(B).
videos have been the subject of DMCA takedown notices regarding uses that are clearly privileged under the fair use doctrine. The uses at issue have been the inclusion of fewer than ten seconds of footage from news broadcasts in campaign ads or videos, as a basis for commentary on the issues presented in the news reports, or on the reports themselves. . . . Despite the complete lack of merit in these copyright claims, YouTube has removed our videos immediately upon receipt of takedown notices. This is both unfortunate and unnecessary. It is unfortunate because it deprives the public of the ability to freely and easily view and discuss the most popular political videos of the day. And it is wholly unnecessary from a legal standpoint.88

YouTube responded that its hands were tied by the DMCA and that it would not play favorites among the many campaign videos posted.89 YouTube also argued that it was simply an intermediary in this exchange and did not have direct access to any critical information regarding copyright ownership and infringement.90 YouTube suggested that McCain could counter-notify or sue, but it would not be possible to have the campaign advertisements restored to YouTube before the expiration of the statutory delay. Finally, YouTube tritely suggested that Senator (or President) McCain could also work to change the law so that others were not ensnared by it in the future.91

This example illustrates a crystal-clear case of fair use regarding speech protected by the First Amendment.92 The concept of safe harbor should never have entered the picture, but YouTube, following standard DMCA policy and in an effort to avoid litigation or further dispute,


90 Id. at 2.

91 Id. at 3.

never examined the legal validity of the underlying copyright complaint.\textsuperscript{93} As long as a copyright holder sends a compliant notice to an ISP, that ISP is required to respond expeditiously to remove the disputed video or risk being targeted for contributory infringement.\textsuperscript{94} Even though the McCain campaign responded with counter-notification asserting non-infringement, the DMCA required YouTube, an ISP seeking safe-harbor protection from liability, to keep the videos offline for seven to ten days.\textsuperscript{95}

All too often, blog posts are redacted, videos deleted, and web pages removed from search results based upon private claims of copyright infringement. The safe-harbor provision of the DMCA encourages service providers to respond to copyright complaints with expeditious takedowns, which assures the ISPs immunity from liability, but also diminishes the rights of their subscribers and users. The law's shield for service providers becomes, paradoxically, a sword against the public, which depends upon these ISPs as platforms for speech.\textsuperscript{96}

There has also been legal debate surrounding the interpretation of the phrase “right and ability to control,” as it is used in the DMCA.\textsuperscript{97} In a recent case, \textit{UMG Recording, Inc. v. Shelter Capital Partner LLC},\textsuperscript{98} the Ninth Circuit pointed out that having the legal right and necessary tools to remove infringing content is not synonymous with having a practical ability to control infringing activity.\textsuperscript{99} The court reinforced its premise with the basic rule that a statute should be

\textsuperscript{93} \textit{DMCA Policy}, \textsc{YouTube}, http://www.youtube.com/t/dmca_policy (last visited August 26, 2013).


\textsuperscript{95} 17 U.S.C. §512(g).

\textsuperscript{96} Seltzer, \textit{supra} note 92, at 175.

\textsuperscript{97} 17 U.S.C. § 512(c)(1)(B).


\textsuperscript{99} \textit{Id.}
interpreted based upon the plain meaning of its text.\textsuperscript{100} The ordinary meaning of the words “ability” and “control” require a controlling party only to possess the necessary powers or resources to do so, not to assert these powers.\textsuperscript{101} Consequently, the Ninth Circuit held, “a service provider must be aware of specific infringing material to have the ability to control that infringing activity within the meaning of the DMCA. Only at that point would its failure to exercise its ability to control deny it a safe harbor.”\textsuperscript{102}

In another recent case, \textit{Hendrickson v. eBay, Inc.},\textsuperscript{103} the United States District Court for the Central District of California came to a similar conclusion regarding the explicit definition of “right and ability to control.” The court explained:

First, the “right and ability to control” the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored in its system. To hold otherwise would defeat the purpose of the DMCA and render the statute internally inconsistent. The DMCA specifically requires a service provider to remove or block access to materials posted on its system when it receives notice of claimed infringement. See 17 U.S.C. §§ 512(c)(1)(C). The DMCA also provides that the limitations on liability only apply to a service provider that has “adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of [users] of the service provider's system or network who are repeat infringers.” 17 U.S.C. § 512(i)(1)(A). Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA.\textsuperscript{104}

\textsuperscript{100} Id.

\textsuperscript{101} Id. at 1041.

\textsuperscript{102} Id. at 1042.

\textsuperscript{103} Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001).

\textsuperscript{104} Id. at 1088.
The district court concluded that an ISP's ability to remove materials posted by third parties did not satisfy the concept of “right and ability to control,” because such power is necessary for an ISP to satisfy the basic requirement of “takedown” under the DMCA.\textsuperscript{105}

The examples above illustrate several types of inconsistencies and confusions surrounding DMCA safe harbors. The McCain example illustrates flaws in the standard implementation of the law, and the far-reaching consequences that have been caused, even outside the cases governed by the DMCA safe harbors. The subsequent case examples, \textit{UMG} and \textit{Hendrickson}, point out the complications that the indistinctness of the actual text of the law has caused. These examples, and the examples provided in the anti-circumvention section of this article, indicate that the judicial system should take action to clarify, at the very least, the major parameters of the law.

\textbf{VII. FUTURE IMPLICATIONS AND POSSIBLE ALTERNATIVES}

A happy medium for both copyright holders and ISPs is not going to be found in rejecting the DMCA in favor of new laws. Laws aimed at policing the state of the Internet are generally not effective, and the protections built into the DMCA are so core to the way the Internet functions that it would not be practical to just “toss a full-grown Internet out with the bathwater.”\textsuperscript{106} Several other options exist that could help alleviate the debate in a more concrete manner. One suggestion for accomplishing this goal is to interpret the law with greater constitutional scrutiny.

When non-infringing speech is taken down, not only does its poster lose an opportunity

\begin{footnotesize}
\begin{enumerate}
\item[\textsuperscript{105}] Id. at 1093-94.
\item[\textsuperscript{106}] Wagner, \textit{supra} note 8.
\end{enumerate}
\end{footnotesize}
to reach an audience, the public loses the benefit of hearing that lawful speech in the marketplace of ideas.\textsuperscript{107} One alternative that may help iron-out varying DMCA interpretations is to treat DMCA safe harbor cases with a greater level of constitutional scrutiny.\textsuperscript{108} The heightened scrutiny can be accomplished by rebalancing speech protection and copyright to reduce erroneous takedown.\textsuperscript{109} Currently, copyright holders are more inclined to send a DMCA takedown notification because it costs less than filing a complaint in federal court and exposes the copyright holder to fewer risks. However, this practice also invites more frequent abuse and error than pursuing the case in court and produces a blander but not significantly less infringing information space.\textsuperscript{110}

Copyright holders assert that the expedited process of the DMCA is critically necessary to suppress infringement in a highly networked and fast-paced digital world. While many instances of infringement are correctly targeted for takedown under the DMCA, the accuracy of some takedowns cannot be an excuse for error in other instances. It also does not excuse the failure to undertake careful examination of the rate and costs of error.\textsuperscript{111} The answer to this debate, and to many legal disputes in general, is to simply give the parties good alternatives.\textsuperscript{112}

\begin{enumerate}
\item[107] Abrams v. United States, 250 U.S. 616, 630 (1919).
\item[109] Seltzer, \textit{supra} note 92, at 171.
\item[110] \textit{Id}.
\item[111] \textit{Id}.
\item[112] Wagner, \textit{supra} note 8.
\end{enumerate}