THE DMCA’S SAFE HARBOR PROVISION: IS IT REALLY KEEPING THE PIRATES AT BAY?

Charles K. Lane†

I. INTRODUCTION ......................................................... 194

II. THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 (DMCA) .......................................................... 195
   A. BACKGROUND ........................................................ 195
   B. SECTION 512: THE SAFE HARBOR PROVISION .......... 195
   C. ANTI-CIRCUMVENTION MEASURES.......................... 197
   D. THE TAKEDOWN PROCEDURE .................................. 198
   E. RAMIFICATIONS OF THE TAKEDOWN PROCEDURE .... 200

III. INTERPRETING THE SAFE HARBOR PROVISION – MP3TUNES ................................................................. 201

IV. THE FUTURE OF COPYRIGHT BATTLES: WAGING WAR IN THE “CLOUD”......................................................... 203

V. PROBLEM, PART 1: CIRCUMVENTION IS TOO EASY .. 204

VI. PROPOSAL, PART 1: SELF-DESTROING FILES...... 204

VII. PROBLEM, PART 2: THE EXISTING TAKEDOWN PROCEDURE BURDENS COPYRIGHT USERS AND SERVICE PROVIDERS ......................................................... 205

VIII. PROPOSAL, PART 2: INDEPENDENT REVIEW BOARD DEDICATED TO EFFICIENT COPYRIGHT DISPUTE RESOLUTION ......................................................... 207
   A. PRE-TAKEDOWN NOTICE FOR THE COPYRIGHT

† B.A. Journalism and Mass Communication, University of North Carolina at Chapel Hill (2011); J.D. Candidate (2014), Wake Forest University School of Law; Notes and Comments Editor, Wake Forest Journal of Business and Intellectual Property Law (2013-2014). The author would like to thank the Editors and Staff Members of the Wake Forest Journal of Business and Intellectual Property Law for their hard work on this Article. He would also like to give special thanks to his parents Derek and Janice Lane and to his family, friends, and advisors for their continuing support, without which this article would not have been possible.
User ........................................................................................................ 207
B. INDEPENDENT COPYRIGHT DISPUTE RESOLUTION
   ENTITY .............................................................................................. 208

IX. CONCLUSION .................................................................................. 210
I. INTRODUCTION

Imagine you’re the captain of a giant cargo ship in the middle of an ocean. Your ship is surrounded by countless other ships, some of which are using the ocean for innocent purposes, such as fishing. The rest are fleets of pirate ships constantly stealing your cargo. Generals of the fleets command their ships from a harbor. You could quickly stop the attacks if only you could take out the generals, but unfortunately your attacks cannot reach the harbor. Instead, you have two attack options – target individual pirate ships (an inefficient use of your resources), or launch massive attacks (running the risk of damaging fishing boats and pirate ships alike).

This is the battle currently being waged over copyrighted material on the Internet. Compare the cargo ship to a copyright holder (e.g., a music record label) and the cargo to the label’s copyrighted material. The maritime pirates, of course, play the role of their brethren of the Internet variety. The fishing boats play the role of legally protected fair users of copyrighted material, and the generals can be equated to Internet service providers who qualify for Digital Millennium Copyright Act (“DMCA”) safe harbor protection.

This scene illustrates the conundrum of copyrighted material on the Internet: a copyright holder cannot protect his copyright until it has been infringed, and a fair user cannot defend his use until it has been inhibited. This article proposes a solution that benefits both the copyright holder and the copyright user, while curbing circumvention of copyright protections. This solution, discussed in depth below, essentially proposes two things: a modification to the anti-circumvention devices actually placed on copyrighted material and an expedited, third party takedown procedure for faster resolutions.

This article will provide background on selected portions of the DMCA addressing safe harbor protection, anti-circumvention measures, and takedown procedures. It will then identify two primary problems with the DMCA: circumvention of copyright protection is too easy, and copyright holders have too much power in the takedown process. Finally, the article will address these two issues with proposed solutions that will benefit all parties involved.

The Internet is a vast area, and copyrights protect expression in many forms. In the interest of precision, this article will focus primarily on copyright protection as it relates to digital audio files to illustrate the current landscape of the safe harbor.
II. THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 (DMCA)

A. Background

Congress passed the DMCA in 1998 in response to growing concerns over copyright protection on the Internet.\(^1\) As the story goes, the Clinton administration desired to strengthen online copyright protection to increase the spreading of ideas on the Internet.\(^2\) Met with resistance at home, the Clinton administration pushed for an international conference on copyright protection.\(^3\) The administration hoped that an international treaty would inspire confidence through international uniformity among copyright holders.\(^4\) In 1996, member nations of the World Intellectual Property Organization (“WIPO”), an agency of the United Nations, gathered to discuss copyright law.\(^5\)

This international conference resulted in two treaties: the WIPO Copyright Treaty (“WCT”) and the WIPO Performances and Phonograms Treaty (“WPPT”).\(^6\) In 1998, Congress codified portions of these treaties in the form of the DMCA.\(^7\) The following two sections discuss the two portions of legislation most relevant to this article: the “safe harbor” provisions and the anti-circumvention measures.

B. Section 512: The Safe Harbor Provision

While Congress passed the DMCA generally to encourage copyright holders to spread information, Section 512 serves an opposite, yet equally important function: to encourage service providers to handle copyrighted material without constant fear of litigation.\(^8\) The DMCA defines a service provider as “an entity

\(^2\) David Robinson, DMCA Week, Part I: How the DMCA Was Born, FREEDOM TO TINKER (Oct. 27, 2008), https://freedom-to-tinker.com/blog/dgr/dmca-week-part-i-how-dmca-was-born/.
\(^3\) Id.
\(^4\) Id.
\(^5\) Id.
\(^8\) Frequently Asked Questions (and Answers) About DMCA Safe Harbor, CHILLING EFFECTS, https://www.chillingeffects.org/dmca512/faq.cgi (last visited continued . . .}
offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received”\(^9\) or “a provider of online services or network access, or the operator of facilities therefor.”\(^10\) Examples of service providers are YouTube, which hosts user-submitted videos,\(^11\) and MP3tunes, which hosts “lockers” where users may store files.\(^12\)

The so-called “safe harbor” provision of the DMCA protects service providers that meet several basic requirements.\(^13\) A service provider may escape liability for hosting infringing material if it:

(A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.\(^14\)

In addition to these requirements, a service provider must notify its users of its policies regarding copyright infringement and follow proper notice and takedown procedures initiated by copyright holders.\(^15\)

---

\(^13\) See CHILLING EFFECTS, supra note 8.
\(^15\) See CHILLING EFFECTS, supra note 8.
C. Anti-Circumvention Measures

Another important facet of the WIPO treaties and the DMCA was the method by which they sought to punish those who attempted to circumvent copyright protection.\footnote{16}{17 U.S.C. § 1201 (2006).} Digital copyrighted works are generally protected by one or both of two kinds of mechanisms: access control and copy control mechanisms.\footnote{17}{Frequently Asked Questions (and Answers) About Anticircumvention (DMCA), CHILLING EFFECTS, https://www.chillingeffects.org/anticircumvention/faq.cgi (last visited Oct. 3, 2013).}

Section 1201 of the DMCA defines an access control mechanism as one that “in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.”\footnote{18}{17 U.S.C. § 1201(a)(3)(B) (2006).} An example of this may be a password, without which an end user cannot access the copyrighted material.\footnote{19}{See CHILLING EFFECTS, supra note 17.}

Section 1201 likewise defines a copy control mechanism as one that “in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner.”\footnote{20}{17 U.S.C. § 1201(b)(2)(B) (2006).} Examples of copy controls include those that “limit what you can do with the work after you have access (e.g., whether you can copy the work, how many copies can be made, how long you can have possession of the work, and the like).”\footnote{21}{Circumventing Copyright Controls, DIGITAL MEDIA L. PROJECT, http://www.dmlp.org/legal-guide/circumventing-copyright-controls (last visited Oct. 3, 2013).}

The act of circumvention of one of these controls means “to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.”\footnote{22}{17 U.S.C. § 1201(a)(3)(A) (2006).} Circumvention in this context equates to the pirates jumping onto your ship and breaking down a locked door before stealing your cargo. The policy rationale underlying Section 1201 reflects the feeling that copyright holders will be more confident spreading information if they can adequately safeguard who uses and copies the information.\footnote{23}{See Robinson, supra note 2.}

The relative ease of circumvention of copyright protection is arguably one of the biggest flaws in the current system. The digital
rights management ("DRM") system illustrates this problem.³⁴ In one common example, a user purchases a song file with an attached encryption key embedded in the file, which works forever.³⁵ The catch is that this encryption key will only decode the file contents when it is accessed from the computer on which it was originally downloaded.³⁶ If the user tries to transfer that song to another device, the encryption key will not decode, and the user will not hear the song.³⁷

This setup seems secure, but the problem arises when a clever user learns how to detach that encryption key from the file, allowing the song to be played on any device. A quick Google search for “DRM removal” shows how many programs have been designed to carry out the basic function of stripping encryption from protected files.³⁸ The flaw in the system is that the song file can exist separately from the encryption key. Consider the cargo ship again – the cargo remains intact after the pirates bust down the door. But what if the removal of the access control ruined the song itself? What if the door had dynamite attached to it that detonated when someone broke down the door, destroying the cargo inside? This solution could prevent a substantial amount of copyright infringement on the front end, with little effort from the copyright holder on the back end of the takedown procedure.

D. The Takedown Procedure

Like the steps to qualify for safe harbor protection, the steps to file an effective DMCA takedown notice are fairly simple. To file such a notice, a copyright holder must give a service provider only the following information:

1. The name, address, and electronic signature of the complaining party.²⁹

2. The infringing materials and their Internet location,³⁰ or if the service provider is an "Information

³⁵ Id.
³⁶ Id.
³⁷ Id.
Location Tool” such as a search engine, the reference or link to the infringing materials.\textsuperscript{31}

3. Reasonably sufficient information to identify the copyrighted works.\textsuperscript{32}

4. A statement by the owner that it has a good faith belief that there is no legal basis for the use of the materials complained of.\textsuperscript{33}

5. A statement of the accuracy of the notice and, under penalty of perjury, that the complaining party is authorized to act on the behalf of the owner.\textsuperscript{34}

Once a service provider receives knowledge of infringing material, through notice from a copyright holder or through its own volition, it must immediately remove the allegedly infringing material to maintain the protection of the safe harbor.\textsuperscript{35} No step in the procedure requires that the service provider verify the status of the alleged copyrighted material.\textsuperscript{36} If a copyright holder meets the requirements above, the service provider will be required to remove the materials immediately or he will face liability.\textsuperscript{37}

The result of the takedown procedure is that any user of copyrighted materials, for any purpose, will face the constant threat of takedown with no notice or opportunity to defend himself. Section 512 does, however, provide a post-takedown remedial procedure for users of copyrighted materials.\textsuperscript{38}

Once a service provider has notified its subscriber that the subscriber’s material has been removed pursuant to a DMCA takedown notice, the subscriber may file a counter-notice.\textsuperscript{39} The subscriber’s counter-notice to the service provider must include:

1. The subscriber’s name, address, phone number and physical or electronic signature.\textsuperscript{40}

\textsuperscript{31} 17 U.S.C. § 512(d)(3).
\textsuperscript{34} 17 U.S.C. § 512(c)(3)(A)(vi).
\textsuperscript{35} 17 U.S.C. § 512(c)(1)(C) (establishing that in order to qualify for safe harbor protection, a service provider must “respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.”).
\textsuperscript{36} See CHILLING EFFECTS, supra note 8.
\textsuperscript{37} Id.
\textsuperscript{38} Id.
\textsuperscript{39} Id.
2. Identification of the material and its location before removal.\(^4\)

3. A statement under penalty of perjury that the material was removed by mistake or misidentification.\(^2\)

4. Subscriber consent to local federal court jurisdiction, or if overseas, to an appropriate judicial body.\(^3\)

Once a proper counter-notice has been filed, the service provider must immediately notify the claiming copyright holder of the subscriber’s objection to the takedown.\(^4\) If the claiming copyright holder does not bring a lawsuit against the subscriber in fourteen days, the service provider must restore the material in question to its original location.\(^5\)

E. Ramifications of the Takedown Procedure

The takedown procedure poses problems for all parties involved. First, the subscriber has no defense before its material disappears. This article sympathizes not with the subscriber who plainly infringes a copyright, but with the subscriber who has a fair use defense to the copyright holder’s takedown claim. A fair user may have amassed hits and commentary on a video or a number of downloads that he stands to lose if a takedown notice removes his material. Whereas the original motivation behind the DMCA was to encourage the dissemination of copyrighted material, this takedown framework seems to discourage fair uses such as commentary and education (though opinions may differ on the deterrence factor of the takedown threat).

Second, the takedown procedure may not be the most efficient way for copyright holders to protect their copyrights. A copyright holder has to file takedown notices for each individual instance of allegedly infringing material. Alternatively, the copyright holder may save time by using a program that identifies the copyrighted material within a search filter, with no distinction between plain infringement and fair use, or even actual ownership of the copyright.\(^6\) This equates to the

\(^{42}\) 17 U.S.C. § 512(g)(3)(C).
\(^{44}\) 17 U.S.C. § 512(g)(2)(B).
\(^{45}\) 17 U.S.C. § 512(g)(2)(C).
cargo ship firing a large blast, eliminating both the pirate ships and the fishermen alike. Even this does not fully benefit the copyright holder: the holder must constantly file individual lawsuits in the short time period after the takedown, and may not wish to litigate every instance of infringement. This situation also presents a moral hazard, because the copyright holder likely values his own copyright more than he values the fair use rights of the individual subscribers.  

Third, the takedown procedure burdens the service provider who, although protected by the safe harbor, must nevertheless act as a conduit between the copyright holder and subscriber. The subscriber may justifiably have a duty to remove infringing material pursuant to a takedown notice; however, it seems inefficient to put the service provider in the role of middleman for counter-notices. A better solution would allow a more accurate determination of the nature of the use of copyrighted material before takedown. This would benefit both the copyright holder and subscriber by providing a degree of certainty, rather than reverting to litigation for every case. It would also benefit the subscriber who stands to have its material removed without warning. The proposed solution discussed below will expand this and other suggestions to expedite the takedown procedure and (theoretically) please everyone.

III. INTERPRETING THE SAFE HARBOR PROVISION – MP3TUNES

In 2011, the United States District Court for the Southern District of New York, in Capitol Records, Inc. v. MP3tunes, delineated what the safe harbor does and does not protect. MP3tunes is a website that allows subscribers to save files in a “locker” hosted on MP3tunes.com. Lockers store three categories of files: those purchased directly from MP3tunes, those uploaded from a subscriber’s

for-abuse-of-anti-piracy-tool-110726/ ("Hotfile has evidence that Warner used an antipiracy tool provided by Hotfile at Warner’s request to improperly remove material for which Warner did not own a copyright, and that Warner removed some material without ever verifying the contents of what it was deleting.").


49 Id. at 633.
personal offline hard drive, and those stored elsewhere on the Internet via hyperlink.\textsuperscript{50} MP3tunes owns and operates a separate website called Sideload.com that allows users to search the Internet for files and save them in lockers via hyperlink.\textsuperscript{51} Both MP3tunes and Sideload.com display an anti-infringement policy and contact information for a registered agent designated to process takedown notices.\textsuperscript{52}

In 2007, EMI, Inc. sent a takedown notice to MP3tunes demanding removal of specific song titles and web addresses, as well as “all of EMI’s copyrighted works, even those not specifically identified.”\textsuperscript{53} Upon request from MP3tunes, EMI refused to specify any more infringing materials, alleging that the information provided was enough to require MP3tunes to remove all infringing material.\textsuperscript{54} These files included files hosted by subscribers who were not parties to this lawsuit and files hosted by MP3tunes founder Michael Robertson.\textsuperscript{55}

The court granted partial summary judgment in favor of both EMI and MP3tunes.\textsuperscript{56} EMI won two summary judgment motions.\textsuperscript{57} The first alleged contributory copyright infringement against MP3tunes and Robertson for songs specifically mentioned in takedown notices that MP3tunes and Robertson failed to remove from user lockers.\textsuperscript{58} EMI’s second successful motion alleged direct infringement against Robertson for “songs he personally sideloaded from unauthorized sites.”\textsuperscript{59}

MP3tunes’ successful motion alleged safe harbor protection for the songs hosted on its website in user lockers.\textsuperscript{60} The court granted this motion with respect to the songs not specifically named in takedown notices.\textsuperscript{61} This holding reinforces the provision in Section 512 that a service provider must have actual knowledge of infringing material before it can be held liable.\textsuperscript{62} The holding makes clear that a service provider must remove all files for which it has actual notice, but is not

\textsuperscript{50} Id. at 633-34.
\textsuperscript{51} Id. at 634.
\textsuperscript{52} Id. at 635.
\textsuperscript{53} Id.
\textsuperscript{54} Id.
\textsuperscript{55} Id. at 650-51.
\textsuperscript{56} Id.
\textsuperscript{57} Id.
\textsuperscript{58} Id.
\textsuperscript{59} Capitol Records, Inc., 821 F. Supp. 2d at 651.
\textsuperscript{60} Id.
\textsuperscript{61} Id.
considered to have actual notice unless a copyright holder specifically lists the files in a takedown notice.

IV. THE FUTURE OF COPYRIGHT BATTLES: WAGING WAR IN THE “CLOUD”

Congress passed the DMCA in 1998 to respond to the changing landscape of copyright law – namely, how to protect copyrights on the Internet. Today, copyright law faces a similar transition. MP3tunes has extra significance and marks the beginning of a shift to cloud-based computing. What differentiates MP3tunes from file-sharing services of the past (e.g., Limewire) is that rather than downloading files to a personal hard drive, users upload files to MP3tunes’ server and can access the files from any Internet-connected device. The last several years have welcomed cloud-based storage services from Apple, Google, Amazon, and others. These services use a controversial process called “deduplication.” Deduplication means that Apple, for example, rather than store multiple copies of the same file uploaded by different users, stores one master copy of the file and allows multiple users to access it. Users can only access files that they already own, but the file they access from Apple’s server is not their own – it belongs to Apple. Companies like Apple find this process beneficial because it greatly reduces the amount of server space they have to maintain. For example, if 500,000 Apple subscribers want to stream a song by Justin Bieber, Apple provides its own copy of the song for all subscribers to access rather than storing 500,000 copies of that song. This process saves Apple roughly 190TB of storage space for that one song alone. For comparison, the storage

63 UC RIVERSIDE, supra note 1.
64 Apple’s website, for example, describes its “iTunes Match” program as a service that “determines which songs in your collection are available in the iTunes Store. Any music with a match is automatically added to iCloud for you to listen to anytime, on any device.” http://www.apple.com/itunes/itunes-match/. For more information on Amazon Cloud Player, visit http://www.amazon.com/b?ie=UTF8&node=2658409011. For more information on Google play, visit https://play.google.com/about. For a comparison of all three services, see Peter Kafka, Google’s Music Locker Now Works Like Apple’s and Amazon’s. Except It’s Free, ALLTHINGSD (Dec. 18, 2012, 10:00 AM), http://allthingsd.com/20121218/googles-music-locker-now-works-like-apples-and-amazons-except-its-free.
66 According to Google, 190.735TB = 195,312.5GB = 200,000,000MB = 4MB * 500,000 (an average song at standard compression rate can be estimated around 4MB).
space of an average consumer external hard drive today ranges from 100GB to 4TB.67

V. PROBLEM, PART 1: CIRCUMVENTION IS TOO EASY

DRM protection can be circumvented in several ways. Two common ways are hacking the DRM encryption (illegal) and making a sound recording of a DRM-protected file (sometimes legal).68 The first method is internal in nature—a user would manipulate the file him or herself. The process of making a sound recording to create a new DRM-free file, on the other hand, is external in nature. Unfortunately, it is virtually impossible to fathom an anti-circumvention measure to combat the user who skirts DRM protection by making a sound recording. The next section focuses on the problem that hacking the DRM encryption is relatively easy, and the audio file still plays normally after the DRM encryption has been hacked.

VI. PROPOSAL, PART 1: SELF-DESTRUCTING FILES

In the “Mission: Impossible” television series from the 1960s, Jim Phelps would receive a top secret mission on a tape recorder concluding with the message: “This tape will self-destruct in five seconds.”69 The tape recorder would then go up in a puff of smoke only 1960s special effects could deliver, rendering the machine unusable and the classified information irretrievable. Copyright protection should make digital audio files similarly irretrievable to pirates, or to return to the recurring metaphor, the cargo should self-destruct when pirates break down the door.

In theory, DRM protection already does exactly this. However, it, unfortunately fails to hold up against circumvention techniques.70 Instead, DRM protection should be adapted to scramble a file in response to a piracy attempt. When a DRM removal tool attempts to

70 See CHILLING EFFECTS, supra note 8 (Noting that the availability of DRM Removal tools online suggests a level of ease to removing DRM protection and using copyrighted material).
unlock a file, the file could scramble itself.

This solution has multiple benefits. First, it only responds to those who attempt to hack the DRM; it does not affect the regular user who uses the file within the parameters of the DRM protection. Second, heightened DRM protection would likely be cost-efficient to the copyright holder. The cost imposed on the copyright holder to implement heightened DRM protection would likely be negated by the revenue saved by preventing DRM stripping. In turn, a reduction in the instances of DRM stripping would likely decrease the quantity of infringing files on the Internet. A lower quantity of infringing files would relieve another burden on the copyright holder because it would reduce the number of DMCA takedown notices the copyright holder needs to file.

VII. Problem, Part 2: The Existing Takedown Procedure Burdens Copyright Users and Service Providers

Copyright users face their own burdens in the existing DMCA system. To recap the DMCA takedown procedure: a copyright holder gives notice to a service provider, who then pulls down files named specifically in the notice. If a copyright user believes the takedown to be unjustified, the user may file a counter-notice. 71 This system treats the fair user and the infringing user exactly the same way; it denies both users the opportunity to defend their respective uses before takedown. Here the means (taking down all allegedly infringing material without notice to the copyright user) is not narrowly tailored to the end (preventing infringement) 72

This process puts enforcement in the hands of the copyright holder, who in some cases may have no vested interest in protecting fair use of its copyright. Unfortunately for copyright users, the DMCA does not require the copyright holder to verify that it holds a copyright to each file it names in a takedown notice. 73 Instead, the DMCA only holds the copyright holder liable for erroneous takedown

72 An online legal dictionary, TransLegal, defines “narrowly tailored” as “to carefully draft laws or make policies to address a specific objective without affecting other rights or the smooth running of business.” TransLegal, http://www.translegal.com/legal-english-dictionary/narrowly-tailored (last visited Oct. 3, 2013).
notices when the copyright holder “knowingly materially misrepresent[s]” its copyright claim.\(^{74}\) This eases the burden on, but invites abuse by, a large-scale copyright holder. This scenario creates the potential for intentional and unintentional bogus takedown notices.

In 2011, file-hosting service Hotfile claimed that Warner Brothers abused the takedown process by removing files from Hotfile that Warner Brothers did not own.\(^{75}\) In court, Warner Brothers confirmed the allegation, admitting that: “given the volume and pace of new infringements on Hotfile, Warner could not practically download and view the contents of each file prior to requesting that it be taken down through use of the SRA tool.”\(^{76}\) Warner Brothers asserted that an overbroad automated search filter erroneously named material Warner Brothers did not own.\(^{77}\)

In addition to unintentional false takedowns, Warner Brothers admitted to purposefully taking down material it did not own.\(^{78}\) In one instance, a Warner Brothers employee took down open-source software designed to “facilitate the rapid downloading of the infringing Warner content.”\(^{79}\) Warner also conceded that it “was not the owner of the software itself.”\(^{80}\)

The Hotfile-Warner Brothers conflict illustrates the imbalance of power in the DMCA takedown process. A copyright holder can take down three kinds of material without notice to the user: infringed material it owns, fairly used material it owns, and material it does not own. All three types of material are subject to immediate removal, even though only the first type deserves to be taken down pursuant to the law. The next section will propose a solution that expedites the process and gives the user an opportunity to defend its use before removal.

\(^{74}\) Id.

\(^{75}\) See Ernesto, supra note 46 (“Hotfile has evidence that Warner used an antipiracy tool provided by Hotfile at Warner’s request to improperly remove material for which Warner did not own a copyright, and that Warner removed some material without ever verifying the contents of what it was deleting.”).


\(^{77}\) Id. ("Warner admits that its records indicate that URLs containing the phrases ‘The Box That Changed Britain’ and ‘Cancer Step Outsider of the Box’ were requested for takedown through use of the SRA tool.").

\(^{78}\) Id.

\(^{79}\) Id.

\(^{80}\) Id.
VIII. PROPOSAL, PART 2: INDEPENDENT REVIEW BOARD DEDICATED TO EFFICIENT COPYRIGHT DISPUTE RESOLUTION

The copyright holder has the upper hand in the current takedown procedure. An ideal solution would bring this power back into balance. That solution needs to address two overarching goals: (1) notify the copyright user before takedown, and (2) put enforcement of takedowns in the hands of an independent entity.

A. Pre-Takedown Notice for the Copyright User

First and foremost, the copyright user must receive notice before the service provider removes the material in question. This move will create its own issues, but no solution can adequately address the shortcomings of the DMCA takedown procedure without it. The copyright holder will notify the service provider, who will then provide notice to the user but take no further action.

This modification has obvious advantages to the copyright user. A fair user finally gains the opportunity to defend itself and keep its material online without a gap. It also protects users from erroneous takedown notices like those discussed in the context of Hotfile and Warner Brothers.

However, this modification taken in a vacuum also presents a new burden to the copyright holder. The time period in which the copyright user may defend its use means more time that infringing material remains online. Therefore, a solution implementing this change needs to retain an element of efficiency. The longer the process takes, the longer a copyright holder must wait to rightfully remove its material from the Internet.

Another issue arises when the nature of the copyrighted material does not clearly specify whether a use should be classified as fair or infringing. In a recent example, Don Henley, a member of American classic rock band The Eagles, threatened a lawsuit against Frank Ocean, a musician who used a sample of the Eagles’ classic song “Hotel California.” Henley did not initiate DMCA proceedings against Ocean, but this example illustrates the gray area in classifying the uses of copyrighted material. This triggers an extensive fair use analysis, which falls somewhat outside the scope of this article. In short, the current DMCA system allows no determination of the type

---

of use involved and treats all uses equally. Therefore, any adequate solution should provide for at least some analysis of the type of use involved before takedown.

B. Independent Copyright Dispute Resolution Entity

The Hotfile-Warner Brothers conflict illustrates how much power the copyright holder can have in the takedown process. The holder determines which files come down, subject to a standard of “good faith” belief. Any adequate solution should remove bias from the determination of which files to remove. This duty would be best suited for an independent entity.

The question then becomes: which entity can make determinations of which files to remove, and how can that entity remain independent? The determinations will affect federal copyright law. Presumably, the authority could only be vested in the federal government, perhaps through an executive branch agency. Such an agency carries with it the opportunity of influence by lobbyists. This would give large-scale copyright holders like record labels significant power over individual copyright users. Therefore, passage of lobbying or donation limitations should accompany the creation of such an agency.

The existence of such an agency has several notable advantages over the current system. First, as previously mentioned, it takes the sole discretion over takedowns out of the hands of the self-interested copyright holder. An independent agency has the ability to determine which files should be taken down based on precedent from existing copyright law. The agency can serve as a mediator between the copyright holder and copyright user.

Second, an agency dedicated to this function would theoretically have the ability to process takedown disputes quicker than a service provider acting as the middleman. This would alleviate some of the concern addressed above that the process would need to operate much quicker if copyright users were to have notice before takedown. Third, by handling all such takedown disputes, the agency could develop a system of precedent, potentially streamlining the process and offering consistency to the files selected for takedown.

Fourth, using that precedent, the agency could offer the equivalent of advisory opinions before or immediately after a takedown request, giving the parties some insight into the likelihood of takedown success. This has the added benefit of reducing the number of claims that go through litigation, thus saving money for all parties, and

---

lightening court dockets. For example, if the agency offered an advisory opinion based on precedent that a particular file should almost certainly be removed, the copyright user would be less likely to fight the takedown notice. In the current system, the implicated user has no guidance on the likelihood of success of a counter-notice.

Significantly, these advisory opinions would not carry the weight of law or any binding agreement. The parties would still have the opportunity to litigate any dispute at their discretion. The goal of this aspect is only to sift out some of the disputes with clear-cut winners. A binding system would introduce a new, tangled web of litigation where disgruntled parties challenge the agency’s advisory opinions, undermining the very goal of this proposal.

Fifth, the agency would make final determinations on takedowns. These orders would dictate whether files in takedown notices are actually to be taken down, and the orders would be binding on service providers to comply. Again, here the parties retain the option to litigate any matter at their discretion. Litigation, however, would take the form of appeals of agency decisions rather than trials settling copyright disputes.

Ideally, this agency would issue its advisory opinions if necessary and make final determinations of takedowns quicker than the current system. This would present several challenges that must be addressed. First, the involvement of the executive branch would inevitably face its share of supporters and detractors. In the current political climate, any expansion of government will not fall on deaf ears. The agency would need to develop credibility as the original decision maker in copyright disputes. Assuming it gained such credibility, staffing the agency would become another tense decision. For one agency to handle all copyright disputes, it would have to employ a large base of workers from entry-level to highly specialized expertise. Certainly in an economy where jobs are at somewhat of a premium, entry-level workers would presumably be easy to find. Would the agency be able to find enough specialized workers to handle all the takedown notices from day one?

One final decision to consider concerns who would make the staffing decisions. Would the President appoint or nominate agency heads; would voters select agency members? Also of concern: would these employees serve terms, or would they arrange employment-at-will agreements? The agency would need to insulate itself from political influence to negate the lobbying advantage of large-scale copyright holders. This raises the traditional concern of political actors: long terms of service invite corruption and discourage democracy, but short terms prevent consistency. Short terms of service for agency employees would potentially undermine the
strength of precedent of copyright dispute resolutions. All of these factors considered point to a preferred solution of at-will employees with limits placed on lobbying and political influence.

In summary, this agency would settle disputes quicker than the current system. It would do so by being dedicated to this sole function of copyright law, and by providing advisory opinions that reduce the amount of litigation. The agency would consist of at-will employees with efforts to insulate the employees from outside political influence.

IX. CONCLUSION

The DMCA has faced heavy criticism since its inception.83 Record companies and large-scale copyright holders welcomed the Act, unsurprisingly, because they lobbied hard for it.84 This lobbying success was a bad omen of what was to come in the enforcement of the DMCA.85 Copyright holders have too much power, and can take down virtually anything.86 Copyright users feel that the free flow of information has become stifled.87

On the other hand, pirates roam the seas in droves, pilfering cargo that rightfully belongs to the cargo ship. Somehow, both sides find themselves unhappy in the wake of the passage of the DMCA. This article has identified several problems to address in the current system. Copyright holders have too much power and often file bogus takedown notices. Copyright users, regardless of the nature of their use, are treated the same in the takedown process. Service providers have the burden of removing any file specified by copyright holders, regardless of who actually owns it, in order to stay within the safe harbor of Section 512. Even though the DMCA contains anti-circumvention provisions, users can routinely get around anti-circumvention measures.

The ideal solution, as discussed above, would create a way for files to self-destruct in response to certain circumvention attempts. It would require notice to copyright users before takedown. It would increase the burden of proof on copyright holders before naming files in a takedown notice. Finally, it would create an independent dispute resolution agency to speed up the process and restore the balance of power, while alleviating the court system of frivolous litigation.

84 Id.
85 Id.
86 Id.
87 Id.