

**Before the
U.S. Copyright Office
Library of Congress**

In the Matter of:

Section 512 Study: Notice and
Request for Public Comment

Docket No. 2015-7

JOINT COMMENTS OF

**AMERICAN ASSOCIATION OF INDEPENDENT MUSIC;
AMERICAN FEDERATION OF MUSICIANS;
AMERICAN SOCIETY OF COMPOSERS, AUTHORS AND PUBLISHERS;
AMERICANA MUSIC ASSOCIATION;
BROADCAST MUSIC, INC.;
CHRISTIAN MUSIC TRADE ASSOCIATION;
CHURCH MUSIC PUBLISHERS ASSOCIATION;
GLOBAL MUSIC RIGHTS;
THE LATIN ACADEMY OF RECORDING ARTS & SCIENCES, INC.;
MUSIC MANAGERS FORUM – UNITED STATES;
MUSIC PUBLISHERS ASSOCIATION;
NASHVILLE SONGWRITERS ASSOCIATION, INTERNATIONAL;
NATIONAL ACADEMY OF RECORDING ARTS AND SCIENCES;
NATIONAL MUSIC PUBLISHERS’ ASSOCIATION;
RECORDING INDUSTRY ASSOCIATION OF AMERICA;
RHYTHM AND BLUES FOUNDATION;
SCREEN ACTORS GUILD – AMERICAN FEDERATION OF TELEVISION
AND RADIO ARTISTS;
SESAC HOLDINGS, INC.; AND SOUNDEXCHANGE.**

**Submitted by Jay Rosenthal, Esq. and Steven Metalitz, Esq.
Mitchell Silberberg & Knupp LLP**

The submitting parties (the “Music Community”), described in Appendix A hereto, are associations and organizations whose members create and disseminate a wide variety of copyrighted musical compositions and sound recordings. The Music Community has fully embraced the digital marketplace as the primary avenue for delivering high-quality content to music fans through a variety of exciting platforms. Collectively, the Music Community represents hundreds of thousands of songwriters, composers, music publishers, recording artists, record labels, studio professionals, and others, who rely on copyright protection for their livelihoods.

I. INTRODUCTION

By many measures, this should be a great moment for the music community.

More music is being enjoyed than ever before by fans around the globe. Fans enjoy music through a plethora of music services that offer consumers abundant choice and unprecedented access.¹ Digital platforms are using music to build and drive their businesses.²

But growing market distortions resulting from the pervasive misuse of the Digital Millennium Copyright Act (“DMCA”)³ by online platforms harm music creators and threaten their ability to succeed and thrive in the future.

The DMCA was supposed to provide balance between service providers and content owners, but instead it provides harmful “safe havens” under which many platforms either pay nothing or pay less than market value for music.

The Music Community’s list of frustrations with the DMCA is long. A broken “notice-and-takedown” system. Toothless repeat infringer policies. Active services mischaracterized as passive intermediaries. Incentives for services to embrace willful blindness instead of preventing known and widespread infringement. The words “representative list” read out of the statute.

DMCA reform is essential to bring about balance. A vibrant and healthy future for the music ecosystem depends on it.

Throughout these comments, we note various issues that should be addressed. We stand ready to work with Congress, the Copyright Office, and other stakeholders to develop practical solutions to these issues and enact comprehensive DMCA reform.

II. EXECUTIVE SUMMARY

Several factors have contributed to the failure of the DMCA to fulfill its purpose. To start, Congress enacted the DMCA in 1998 when dial-up Internet speeds and static web sites predominated. Soon thereafter, individuals could be worldwide publishers of content on peer-to-peer networks and service providers began to distribute massive amounts of content uploaded to their servers. And then came along more sophisticated search engines, social networks, and an explosion of smartphones and other mobile Internet access devices. The rules for service providers and tools for content creators set forth in the DMCA proved unsuitable for this new world.

¹ See whymusicmatters.com for a non-exclusive list and description of digital music services available in the United States.

² *Music Fuels the Internet*, RIAA, <http://www.musicfuels.com/>.

³ Unless otherwise stated, all references are to Title II of the DMCA, the Online Copyright Infringement Liability Limitation Act, which added Section 512 to Title 17, U.S. Code.

For example, the notice-and-takedown system has proved an ineffective tool for the volume of unauthorized digital music available, something akin to bailing out an ocean with a teaspoon. There is no evidence that Congress anticipated that Google or any service provider would receive and be required to respond to more than one billion takedown notices.⁴ Google wears this as a badge of honor, yet this fact emphasizes the failure of the DMCA to address the challenges faced by content owners today.

Given all of these fundamental changes, a law that might have made sense in 1998 is now not only obsolete but actually harmful. The problem is compounded by the fact that, as courts, too, have struggled to apply this outdated law for the present day, DMCA has been shifted from its original intent through a series of judicial rulings to strip away adequate protection for content owners.⁵ To start, courts have expanded application of the safe harbors well beyond the passive service providers of 1998 to more active distributors of music that compete directly with services that must obtain licenses. The result: a Hobson's Choice for content owners, either to license content for much less than it's worth, or have the broken notice-and-takedown system as the only recourse. Is it any surprise that in this distorted marketplace revenue from sales of vinyl records outpaces revenue from on-demand, ad-supported video platforms making billions of transmissions annually?⁶

Courts have also given little meaning to key provisions for content owners in the DMCA bargain. Examples include "red flag" knowledge, repeat infringer policies and representative lists. The result: safe harbor status for services that choose to stick their heads in the sand rather than do their fair share, forcing content owners to divert valuable resources from away creating content to sending minimally effective take down notices, or for content owners with limited resources, to actually refrain from sending takedown notices at all. Content owners, especially those with limited resources, simply cannot take on the entire digital universe alone.

At its worst, the DMCA safe harbors have become a business plan for profiting off of stolen content; at best, the system is a de facto government subsidy enriching some digital services at the expense of creators. This almost 20 year-old, 20th Century law should be updated.

⁴ *Google Asked to Remove 100,000 'Pirate Links' Every Hour*, TORRENTFREAK (Mar. 6, 2016), <https://torrentfreak.com/google-asked-to-remove-100000-pirate-links-every-hour-160306/> (estimating that Google will have to process a billion reported links this year alone, a milestone which previously took over a decade to reach).

⁵ Please see responses to Questions 5, 14, 19, 24 and 25 for a discussion of judicial interpretations of these provisions.

⁶ Cary Sherman, *Valuing Music In a Digital World*, FORBES (Sept. 23, 2015), <http://www.forbes.com/sites/realspin/2015/09/23/how-government-set-licensing-killed-the-music-industry/#23d7a29cf988>; see also Cary Sherman, *State of the Music Business: What the Numbers Tells Us*, RIAA (Mar. 22, 2016), <https://medium.com/@RIAA/state-of-the-music-business-what-the-numbers-tell-us-63ce1524b30#.wcdv03wso>; RIAA 2015 Year-End Sales & Shipments Data Report, available at <http://www.riaa.com/reports/riaa-2015-year-end-sales-shipments-data-report-riaa/>.

III. GENERAL EFFECTIVENESS OF SAFE HARBORS

To supplement the Music Community's answers to the questions below, we have attached, as Appendix B, a detailed history of the pre-DMCA legal and economic ecosystem, including analysis of the cases and political history related to the passage of the DMCA.

1. Are the Section 512 safe harbors working as Congress intended?

In a word, NO. When it passed the DMCA in 1998, Congress intended to provide effective protection for copyright owners while allowing for the continued growth and development of the Internet. It intended to find a balance: limit liability for certain classes of passive service providers in exchange for effectively addressing infringement. Yet, today, digital services enjoy an (expanding) safe harbor while content owners face an increasing onslaught of digital infringement, with no effective recourse. This couldn't possibly be what Congress meant to achieve.

To better understand Congress's intent, it makes sense to recall the online experience of the late 1990s. When the DMCA was enacted, Internet access was slow; online material was difficult to locate; consumers in many countries lacked widespread access to the Internet; Internet businesses (including access providers, hosts, and website operators) largely earned income from subscription or use-based pricing; and computing devices were expensive and stationary.

Given Congress's understandable inability to anticipate the dramatic transformation of the Internet, the DMCA has failed to scale, rendering it increasingly obsolete and futile from an enforcement standpoint. Consider that, since 2012, the Recording Industry Association of America ("RIAA") has sent more than 175 million infringement notices in the aggregate to web site operators, their underlying hosting providers, and search engines. Many of these relate to works taken down on a particular site, only to see a repeat infringement of the same work appear on the same site.⁷ And then, that repeat infringement is often once again indexed by search engines. This is of particular concern as search engines are one of the leading ways to discover pirated music.⁸ This renders the notice-and-takedown process minimally effective at best.

Of course, what is expensive and difficult for large copyright owners is an impossible task for small copyright owners seeking to protect the value of their works.⁹ As described in response to Question 8, Maria Schneider, a three-time GRAMMY winning jazz and classical composer, bandleader and conductor noted in describing her frustration with the DMCA, "[t]he DMCA makes it my responsibility to police the entire

⁷ Please see responses to Questions 6 and 7 for examples of such repeat infringements.

⁸ Source: Survey of digital music listeners by consumer research firm MusicWatch; Russ Crupnick, *Bad Company, You Can't Deny*, MUSICWATCH (Feb. 22, 2016), <http://www.musicwatchinc.com/blog/bad-company-you-cant-deny/>.

⁹ See Nelson Granados, *How Online Piracy Hurts Emerging Artists*, FORBES (Feb. 1, 2016), <http://www.forbes.com/sites/nelsongranados/2016/02/01/how-online-piracy-hurts-emerging-artists/#488ccf0a7fa2>.

Internet on a daily basis. As fast as I take my music down, it reappears again on the same site—an endless whack-a-mole game.”¹⁰ ESL Music and Thievery Corporation co-founder Eric Hilton has stated even more distinctly “if our music was taken down, it would almost immediately return on another site or even the same site. We were spending more and more resources on the takedown notices, and we were consistently getting less and less in return. Eventually, we decided to stop sending the notices altogether. It was simply an exercise of throwing good money after bad. So time and again, we released product realizing more and more that we had no real way to stop its unauthorized use and the erosion of its commercial viability.”¹¹

Unfortunately, large, sophisticated entertainment-oriented digital services have thrived as a result of this “whack-a-mole” process, premising business models on being shielded from responsibility by the safe harbors. As filmmaker Ellen Seidler asks, “Why does Google make it so damn difficult to send a DMCA notice?” She provides a step-by-step guide on takedown notices, with all the pitfalls and roadblocks set up by Google and writes, “Google has designed cutting edge online tech, but its DMCA procedures are something out of the Dark Ages. That’s no accident.”¹²

So what was the proper balance Congress sought in 1998? Congress understood that unchecked Internet-based infringement would damage copyright owners.¹³ Congress intended to retain for copyright owners the kind of “effective – not merely symbolic – protection” it had always provided for their property.¹⁴ Congress sought a balance by providing liability limitations to service providers that acted responsibly to help achieve the Internet’s potential. However, Congress certainly did not plan to sacrifice the health of America’s creative industries on the altar of the Internet’s success. Congress specifically did not adopt, as it did with respect to almost all other torts in the Communication Decency Act (“CDA”) two years earlier,¹⁵ blanket immunity for service providers.

Congress was clearly influenced by the existing legal landscape and the dominant views expressed in *Netcom* and its progeny.¹⁶ Importantly, Congress did not intend to absolve service providers of all liability so long as they responded to notices from copyright owners that identified specific infringing items. Instead, Congress’s approach was intended to: (i) preserve direct liability for service providers who actively engaged in infringing conduct, such as selectively choosing which user uploads to repackage and

¹⁰ See Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intell. Prop. and the Internet of the H. Comm on the Judiciary, 113th Cong. 57 (2014) (statement of Maria Schneider).

¹¹ ESL Music Letter, Appendix E. See also individual submission of MusicNotes on challenges faced with the notice-and-takedown system in connection with sheet music.

¹² Ellen Seidler, *Why does Google make it so damn difficult to send a DMCA notice?*, VOX INDIE (Feb. 24, 2016), <http://voxindie.org/why-does-google-make-it-so-damn-difficult-to-send-dmca-notice/>.

¹³ See also “The Law and Policy Landscape Pre-DMCA”, Appendix B, at 11-12.

¹⁴ Report of the Senate Committee on the Judiciary on S. 2037, the Digital Millennium Copyright Act, S. Rep. No. 105-190 (1998); see also Appendix B, at 10-11.

¹⁵ 47 U.S.C. § 230; see also Appendix B, at 7-12 (discussing the various limitations on the immunity for service providers).

¹⁶ *Religious Tech. Center v. Netcom On-Line Comm.*, 907 F. Supp. 1361 (N.D. Cal. 1995) (“*Netcom*”); see also Appendix B, at 8.

make publicly available; (ii) preserve contributory liability for service providers who substantially contributed to infringement while possessing knowledge of facts from which a reasonable person would deduce that infringement is occurring, unless the service provider took steps to stop the infringement upon obtaining such knowledge; and (iii) preserve vicarious liability for service providers who used infringing content to attract or retain users to their websites or networks (*i.e.*, where the value of the product or services was derived in part from access to infringing content) or charged users specific fees associated with infringing content. In short, the DMCA’s approach was intended to create safe harbors only for “innocent” actors.¹⁷

Congress was aware of arguments that it might be difficult for service providers to determine whether content transmitted by users qualified as infringing. Nevertheless, Congress believed that, in many cases, service providers “know infringement when they see it,”¹⁸ and concluded that service providers have a responsibility to take steps to prevent such conduct or risk full liability. When users post copies of recognizable works with recognizable copyright owners or aggregate infringing material and label it as such, services should act.

Of course, too many service providers do not proactively respond to infringement. Judicial decisions have further bolstered this skewed view of liability and responsibility. Courts have repeatedly required less and less – sometimes almost nothing – from Internet intermediaries, and more and more from the content owner. This was never Congress’s intent.

Note that Congress also believed that termination of access to a particular digital service was a reasonable method of deterring repeated copyright violations from persons who flagrantly abused their access in order to violate copyright law. It underscored the importance of this remedy by requiring *all* service providers to implement such methods if they wished to benefit from *any* of the four statutory safe harbors.¹⁹ Yet termination remains a particularly rare occurrence.

It is no surprise that the 2001 European Union E-Commerce Directive that established safe harbors similar to the safe harbors established by the DMCA is also currently under review within the European Union. Commenters there have criticized the Directive as similarly inapplicable to and ineffective in today’s digital marketplace, finding that it unfairly protects and advantages service providers at the expense of music and other rights holders.²⁰

Sadly, it is now clear that the explicit warning sounded in 1995 by the USPTO Working Group’s White Paper has been fulfilled: the safe harbors have “encourage[ed]

¹⁷ *ALS Scan v. RemarQ Communities, Inc.*, 239 F. 3d 619, 625 (4th Cir. 2001).

¹⁸ See Senate Judiciary Committee Report, S. Rep. No. 105-190, 49 (1998).

¹⁹ 17 U.S.C. § 512(i)(1)(A).

²⁰ See European Commission, *Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*, DIGITAL SINGLE MARKET (Sept. 9, 2015), <https://ec.europa.eu/digital-agenda/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud>.

intentional and willful ignorance” on the part of service providers and “chok[ed] the development of marketplace tools that could be used to lessen ... the risk to copyright owners, including ... educating subscribers about infringement and using technological protections, such as tracking mechanisms.”²¹

2. Have courts properly construed the entities and activities covered by the Section 512 safe harbors?

For the most part, courts have *not* properly construed the entities and activities provisions covered by the Section 512 safe harbors.

As an initial matter, courts have generally construed the definition of “service provider” and the “activities” permissible under the safe harbors too broadly. Parties that are nothing like the passive, neutral online service providers that Congress had in mind when drafting and enacting the DMCA now take unfair advantage of the safe harbors. The safe harbors are relied upon by digital services that expressly attract users by hosting and publishing content and directly benefit from such increased user base by mining data and selling advertisements. What was intended to be a limitation on monetary damages for infringing activity by passive, neutral intermediaries has instead become a “get out of jail free” card for all but the most egregious actors.

Although some early cases seemed to recognize that Congress wanted judges to approach cases of online infringement pragmatically,²² too many courts have now diverged from this view.²³ Cases involving YouTube and Veoh exemplify the problem. Consider the following:

- Both services facilitated user access to videos uploaded by third parties and generated revenue by displaying advertising alongside videos;²⁴

²¹ See Appendix B, at 2.

²² See, e.g., *A&M Records, Inc. v. Napster, Inc.*, 54 U.S.P.Q.2d 1746 (N.D. Cal. 1998); *A&M Records, Inc. v. Napster, Inc.*, 2000 U.S. Dist. LEXIS 6243 (N.D. Cal. 2000); *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (N.D. Cal. 2000); *A&M Records, Inc. v. Napster, Inc.*, 239 F. 3d 1004 (9th Cir. 2001).

²³ One reason for this may be the courts improperly grafting principles behind the Communications Decency Act (CDA) onto the DMCA. See, e.g., *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001); *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914 (C.D. Cal. 2003); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004). These cases embody judicial willingness to read the carefully crafted safe harbors too broadly so as to cover conduct, such as facilitating sales of merchandise, that the statute was never designed to protect. Later, poorly conceived claims involving Google’s search engine activities would also lead to broad pronouncements unfairly expanding the safe harbors beyond the four corners of the statute. See *Field v. Google Inc.*, 412 F. Supp. 2d 1106 (D. Nev. 2006); *Parker v. Google, Inc.*, 422 F. Supp. 2d 492 (E.D. Pa. 2006). Courts also sometimes conflated the principles beyond the CDA with those behind the DMCA, not recognizing key differences. See, e.g., *Perfect 10, Inc. v. CCBill, Inc.*, 488 F.3d 1102 (9th Cir. 2007); see also *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003) (“The Digital [Millennium Copyright] Act includes immunity provisions, similar to those of the Communications Decency Act.”).

²⁴ See *Io Grp., Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1143 (N.D. Cal. 2008); *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1117-18 (CD. Cal. 2009) (“*Veoh*”), *aff’d* *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1014 (9th Cir. Cal. 2013); *Viacom, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 528-29 (S.D.N.Y. 2010) (“*Viacom*”), *aff’d in part and*

- Both generated massive traffic to their websites by hosting infringing material, and the court found they had “welcomed” infringing material on their services and advertised its availability.²⁵ Nevertheless, the district courts placed the entirety of the burden of identifying and noticing infringement on copyright owners.²⁶
- In *Veoh*, the court extended the safe harbor even though Veoh was informed that any music videos containing performances by certain listed recording artists were infringing, thereby reading the “representative list” language out of the statute.
- In *Viacom*, the district court decided that liability could attach only if YouTube had knowledge of each specific infringing clip.²⁷
- The court found that YouTube did not have the “right and ability to control infringing activity” even though the service’s founders decided to take down certain types of infringing content, such as full length films, and allow others to remain, including music videos.
- YouTube also had the capability of using digital fingerprinting to block infringing material, but chose to do so only when the content providers entered into licensing agreements with it.²⁸ The court sanctioned this behavior, ruling that the DMCA did not require YouTube to use this software to attempt to stop, for example, repeat postings of a video that had already been identified as infringing through a notice-and-takedown procedure.²⁹

These are but two examples that illustrate how the scales have tilted well beyond the balance Congress sought to create when passing the DMCA.³⁰

Such decisions also ignore how the technological tools available to digital services to prevent or limit systematic infringement have advanced.³¹ When commercial digital services rely on third party content to expand their user base and generate revenue,

remanded, Viacom, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (“*Viacom II*”), *on remand Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 115 (S.D.N.Y. 2013) (“*Viacom III*”).

²⁵ William Hensley, *Copyright Infringement Pushin’: Google, YouTube, and Viacom Fight for Supremacy in the Neighborhood that may be Controlled by the DMCA’s Safe Harbor Provision*, 51 IDEA 607 (2011) (“YouTube’s business model was designed to maximize the number of site viewers in order to increase advertising revenue to attract a buyer. To increase the number of viewers, they needed infringing material.”).

²⁶ *Viacom*, 718 F. Supp. 2d at 528-29.

²⁷ *Viacom III*, 940 F. Supp. 2d at 115. This decision astoundingly applauded the “wisdom of the legislative requirement” that places the burden on the copyright owner to identify and give notice of each infringement, and cited Viacom’s 100,000 takedown notices to YouTube in a single year as evidence that this “system is entirely workable.” *Id.*

²⁸ *Id.* at 119-120.

²⁹ *Id.* at 120.

³⁰ See also responses to Questions 14, 19 and 21 for discussion of erroneous decisions.

³¹ Please see responses to Questions 11 and 15 for a discussion of these technologies.

those services should not be able to avail themselves of the safe harbors simply because they use the public to populate the content on their sites and refuse to implement commercially available tools to weed out unlicensed third party copyrighted content. The DMCA must be rebalanced to address this fundamental unfairness.

3. How have Section 512's limitations on liability for online service providers impacted the growth and development of online services?

The DMCA has hurt the growth of legitimate services that are forced to compete with unlicensed services that use the safe harbors as a shield. Unfair competition impedes the marketplace. Here, unfair competition comes in two forms: completely unlicensed services; and services that negotiate “in the shadow of the law” to obtain below market rates. This distortion in the market stifles investment and ultimately reduces innovation and diversity of services and business models.

Again, the culprits are a variety of problems with the way the DMCA has worked in practice:

- Court interpretations that encourage user-generated content services to turn a blind eye to infringement rather than providing incentives for cooperation;
- A mindset of “use third party copyrighted works first, ask for a license later.”³² Consider that Flipagram, YouTube and SoundCloud all claimed safe harbor status in their early years while relying on music for their growth, and only sought licenses for music after they had obtained substantial audiences.
- Rogue services design and engineer their systems to make the DMCA irrelevant and ineffective in stopping their ongoing infringement. Consider Grooveshark, which profited from its infringing activity for years under the color of the DMCA safe harbor before ultimately being found liable for willful copyright infringement.³³

A balanced law would deter rogue actors from seeking to realize short term profits from music at the expense of music creators, owners, and legitimate digital services. Fixing the DMCA will help legitimate digital services flourish.

³² See Kurt Wagner, *Why Aren't More People Talking About Flipagram? (Q&A)*, RECODE.NET (Mar. 13, 2016), <http://recode.net/2016/03/13/why-arent-more-people-talking-about-flipagram-qa/> (quoting the CEO of Flipagram as saying, “we kind of just did it and [decided] we’d ask for permission after”).

³³ *Capitol Records, LLC v. Escape Media Group, Inc.*, 2014 U.S. Dist. LEXIS 183098, *76-79 (S.D.N.Y. May 28, 2014), *adopted* 2015 U.S. Dist. LEXIS 38007, *18-19, 30-32 (S.D.N.Y. Mar. 25, 2015) (“*Grooveshark*”).

4. How have Section 512’s limitations on liability for online service providers impacted the protection and value of copyrighted works, including licensing markets for such works?

In addition to hampering the growth of other digital music services that choose to partner with the Music Community and license music content, Section 512’s limitations on liability for digital service providers have negatively impacted the protection and value of copyrighted works, including licensing markets for such works in a number of ways:

- Overall protections are limited as the safe harbor allows for many variations of unauthorized use with no meaningful remedy, thus depressing the licensing market.
- The shadow of the safe harbor too often leads to a below market rate.
- When service providers decide to exploit music but not license it and instead hide behind the safe harbor wall, no monetary compensation is offered to content owners, who must also expend resources to identify infringements and send takedown notices.

Rather than encouraging cooperation between service providers and content owners to address infringement, the DMCA has led to certain service providers actively avoiding any knowledge of what is occurring on their service, declining to use readily available tools to limit infringements, and using flawed interpretations of the DMCA to avoid ensuring that works that have been noticed as infringing do not reappear on their service. By way of example, unauthorized uses of One Direction’s “Drag Me Down” reappeared over 2,700 times on YouTube following the first notice.³⁴ The problem is endemic in today’s Internet environment.³⁵ In addition, some social media networks invoke the safe harbors while enabling their users to shield their content from public searching – further impeding the enforcement of copyright rights.

Moreover, rogue actors design their systems to purportedly comply with the DMCA notice-and-take down regime, while actively encouraging infringing behavior, all under the color of the DMCA. As noted above, despite Grooveshark being ultimately found liable for copyright infringement for its egregious behavior,³⁶ it was able to profit from unauthorized use of music for years while the case was litigated. In that case, the court found that Grooveshark had created a “technological Pez dispenser” that required copyright owners to submit “successive takedown notices” in order to remove a single sound recording from the service.³⁷ This “actively prevented copyright owners from

³⁴ IFPI submission on regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy (Dec. 2015).

³⁵ Please see responses to Questions 6-12 for further examples of the DMCA’s failure as a regime to protect copyrighted works.

³⁶ *Grooveshark* at *102-03.

³⁷ *Grooveshark* at *19.

being able to issue meaningful DMCA takedown notifications.”³⁸ Others are so shameless as to publicly tout their activity and seek crowd sourced funding for their illegal efforts.³⁹

This type of brazen work-around of the DMCA by Grooveshark and other rogue actors of the DMCA devalues music and suppresses the legitimate market for it.

Furthermore, the deficiencies in the DMCA, compounded by flawed judicial interpretations of the DMCA has created a “culture of free” mentality, leading to market distortions. As IFPI explained, services directly licensed on the basis of full exclusive rights generated over \$1.3 billion for the music industry in 2014, whereas by comparison, the over 900 million music users of user-uploaded, on-demand streaming platforms generated less than half of that (approx. \$530 million) in the same year.⁴⁰ Based on available data, IFPI estimates that in 2014 YouTube paid out approximately \$0.72 per user per year to record companies, while in 2013 Spotify paid out \$20 per user (no equivalent 2014 data available).⁴¹ “The notice-and-takedown system—intended as a reasonable enforcement mechanism—has instead been subverted into a discount licensing system where copyright owners and artists are paid far less than their creativity is worth.”⁴²

³⁸ *Id.* at *21-22.

³⁹ A particularly egregious example was Aurous, a service that allowed users to search for, stream, and download pirated copies of popular music, and which was designed specifically to search for and retrieve copies from online sources notorious for offering pirated music. Aurous had promoted itself by linking to articles that call it “BitTorrent Music for Your Dad” and “Popcorn Time for Music”; in other words, as a site that made it incredibly easy to find and stream or download pirated music. Aurous brazenly began a crowdfunding campaign for its mobile app. *See* Aurous, “We need your help to bring Aurous to Iphone, Android and Windows phone! Please consider donating to our Indiegogo...”, TWITTER (Sept. 17, 2015, 11:55 am), <https://twitter.com/aurousapp/status/644585368440938496?lang=en>; Aurous, “Hey everyone who contributed to our @Indiegogo campaign, we’ve issued refunds for all our backers, Aurous will be released October 10th.”, TWITTER (Sept. 19, 2015, 1:00 pm), <https://twitter.com/aurousapp/status/645326516600086528?lang=en>. The RIAA, on behalf of its members, brought suit against Aurous, securing a judgment and permanent injunction that shut down the service. *See Atlantic Recording Corporation et al. v. Andrew Sampson*, Case No. 1:15-cv-23810 (S.D. Fla., filed Oct. 13, 2015); Judgment and Permanent Injunction, *id.* (Dec. 23, 2015).

⁴⁰ IFPI submission, *supra* n. 34.

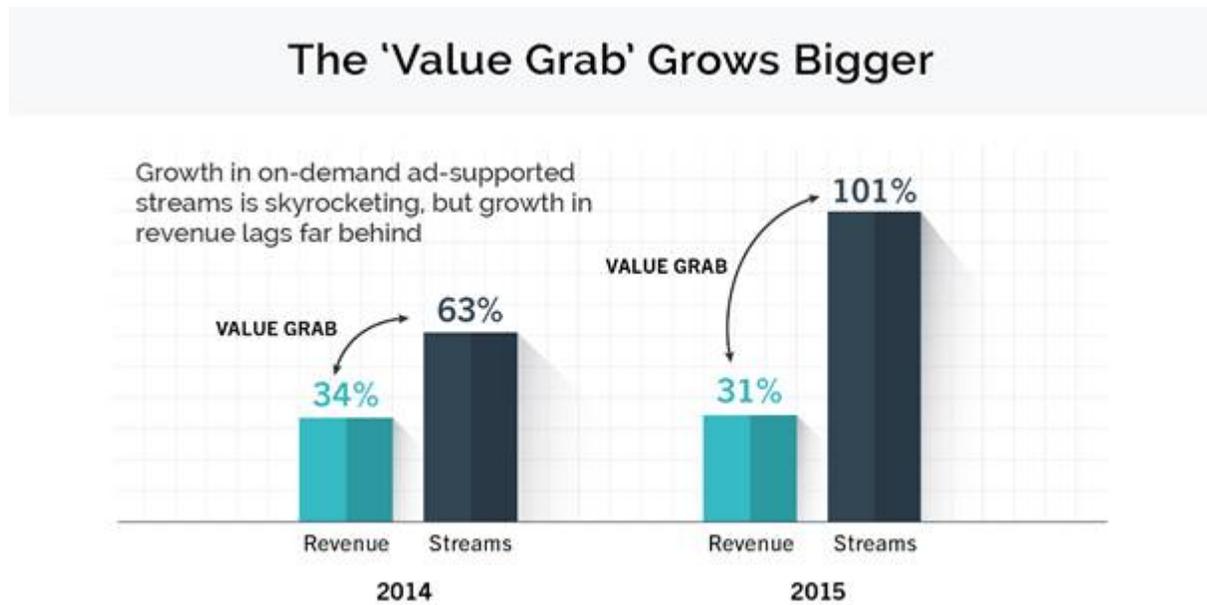
⁴¹ *Id.*

⁴² *See* Sherman, *supra* n. 6; *see also* IFPI submission, *supra* n. 34 (“[O]ur member companies, as content producers, are unable to negotiate fair commercial contractual terms with some online platforms, specifically those that rely on user-uploaded content (‘UUC’), such as YouTube, Dailymotion and SoundCloud. These services build up a user base off the back of UUC content, relying on the lack of clarity in the legal framework, and then make a “take it or leave it” offer. Music companies can license their content on the terms of offer, or not agree to license, knowing that in such case their content will still be available and that they will have no option other than engaging in notice-and-takedown procedures which are ultimately ineffective in handling the vast volumes of UUC. This leads to licenses being concluded at artificially low rates, causing a “value gap” between the income generated by such services from their use of music, and the revenues that are being returned to record companies and artists. This behavior harms creators and producers as well as other music services, consumers, and the economy as a whole.”).

Despite music being more popular than ever today,⁴³ U.S. music industry revenues have been virtually flat since 2010 and are down nearly 50% since the DMCA was enacted in 1998. This has led to what we call the “value grab”, creating market distortions that lead to bizarre statistics like vinyl records generating more revenue for the industry in 2015 than the billions of on-demand ad-supported music streams on YouTube and similar services.⁴⁴

This is further illustrated by the disparity between the annual growth of usage compared with revenues from on-demand ad-supported music streaming in the U.S. This category of music listening includes many popular services such as YouTube, Vevo, the free portion of Spotify, and other services as well.

Chart 4.1 – Disparity between growth in music streaming consumption versus growth in revenues from that streaming consumption



As shown in Chart 4.1, in 2014, on-demand, ad-supported streaming usage grew 63%, while revenues for sound recordings from that usage only grew 34%. This disparity – an indicator of the “value grab” – grew even wider in 2015. In 2015, on-demand, ad-

⁴³ “Demand for music online is higher than ever, with many sites directly dependent upon professionally produced, copyrighted music for their success. Over 65% of Americans ages 13+ agree that music is important to their lifestyle. American consumers spend, on average, more than 24 hours per week listening to music and, in a typical week, 75% of U.S. consumers listen to music online. Twelve of the top 20 most followed people on Twitter are from the Music Community. Fifteen of the top 20 celebrities on Facebook are musicians.” Music Community Written Submission Regarding Development of the Joint Strategic Plan on Intellectual Property Enforcement, in response to Request of the U.S. Intellectual Property Enforcement Coordinator for Public Comments, 80 Fed. Reg. 52800 (Oct. 15, 2015), Appendix C.

⁴⁴ At retail in the U.S., vinyl revenues outpaced revenues from all on-demand, ad supported music streaming services. See Sherman and RIAA 2015 Year-End Sales & Shipments Data Report, *supra* n. 6. Even at wholesale in the U.S., vinyl revenues outpaced revenues from total on-demand, ad supported music video steaming services.

supported music streaming consumption more than doubled in the U.S., while the revenues to the sound recording industry from that usage only grew 31%.

The fact is that, while the technology industry is benefitting from the increased availability of digital music, and profiting from the unprecedented consumption and interest in music, the Music Community is facing a shortfall.

The DMCA has prevented the Music Community from receiving its fair share of the significant and growing digital marketplace.⁴⁵ If the Music Community is to be successful through, creating, investing in, and rewarding music creators, it needs a digital marketplace operating in a free market that properly compensates creators and content owners.

5. Do the Section 512 safe harbors strike the correct balance between copyright owners and online service providers?

The DMCA Section 512 safe harbors may have initially been designed to provide a balanced approach. But after years of transformative technological developments and flawed judicial interpretations of what activities should be permitted to fall within the safe harbor (*i.e.*, what constitutes red flag knowledge, what qualifies as a representative list, etc.),⁴⁶ the DMCA no longer strikes the balance intended by Congress between copyright owners and service providers.

Significantly, broad judicial interpretations of “online service provider” have resulted in safe harbors protecting more than just passive and/or neutral, “innocent” service providers. The unbalanced safe harbors are now relied upon by digital services to attract visitors by hosting content. These services then benefit financially from mining data from, and selling advertisements based on, that increased audience. Some of these services then negotiate with content providers for licensing fees at below market rates (if any fees are paid at all), because the content owners’ only other option is a notice-and-takedown regime that simply does not work.⁴⁷

Some judicial decisions have dis-incentivized service providers from even taking steps to meaningfully stop infringement lest they be deemed to have red flag knowledge of infringement or discover the existence of repeat offenders. This makes service providers actively avoid doing otherwise reasonable things.

Initially Congress sought balance so that Section 512 limitations would enable a nascent online industry. However, given the flawed judicial interpretations of the DMCA, and the incredible growth and market power of this industry, protecting service providers that act as content distributors at the expense of creators is not a justifiable

⁴⁵ See David Israelite, *NMPA Head Says “Free” May Work For Pandora But is Devastating to Songwriters: Op-Ed*, BILLBOARD (Sept. 24, 2015), <http://www.billboard.com/articles/business/6707834/nmpa-david-israelite-oped-pandora-songwriter-payments>.

⁴⁶ Please see responses to Questions 2, 4, 19 and 21 for a more detailed discussion.

⁴⁷ Please see responses to Questions 3 and 4.

policy objective. Instead of enabling certain service providers to unfairly benefit from their exploitation of music, Congress should seek to create a level playing field.

IV. NOTICE-AND-TAKEDOWN PROCESS

6. **How effective is Section 512's notice-and-takedown process for addressing online infringement?**

Section 512's notice-and-takedown process, as implemented, is impracticable and ineffective on today's Internet. Music trade associations have sent notices of over 280 million infringements to Google alone.⁴⁸ Individuals and small-businesses which cannot afford such an undertaking are left without even this minimal protection under the DMCA against digital piracy.⁴⁹ These issues are exacerbated by the "whack-a-mole" nature of the notice-and-takedown process.⁵⁰ Certain service providers have been known to contribute to this problem by ignoring the rampant infringing activity occurring on their sites, and waiting to act until they receive copyright-owner notifications.⁵¹ These notifications may never come because of content owners' unawareness of infringement, or may only come once the infringement has gone viral.⁵² The DMCA was not intended to enable or allow service providers to profit from such widespread and repeat infringement, while shielding themselves from liability; yet it is doing just that.

Music has been particularly hard hit. To get a sense of the scope of the problem, consider that since 2012, RIAA alone has noticed over 175 million infringements of music. In just the short period between the Grammy nominations (December 7, 2015) and the Grammy awards (February 16, 2016), nearly 4,000 unique infringing links were noticed to digital services for just the five nominated "Record of the Year" tracks.⁵³

In addition, there has also been escalating damage from the unauthorized dissemination of pre-release music, *i.e.*, albums slated for commercial release that have not yet been commercially released to the public.⁵⁴ In these circumstances, the

⁴⁸ Source: Google Copyright Transparency Report for infringements noticed by RIAA, BPI, and IFPI.

⁴⁹ See also Granados, *supra* n. 9. Kimberly James, President of indie label CBM, says that within two hours of releasing music, that often costs thousands of dollars to produce, she has found it illegally downloaded on hundreds of websites. Once the music has been uploaded, it's a massive battle to get it taken down, one that most emerging artists cannot afford; a conservative estimate puts 10% of music royalties as lost to piracy.

⁵⁰ Please see response to Question 4 and discussion above.

⁵¹ See *Veoh Networks*, 586 F. Supp. 2d 1132; *Viacom II*, 676 F. 3d at 32-34.

⁵² Brief for Recording Indus. of America Assoc. et al. as Amici Curiae, p. 5, *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500 (S.D.N.Y. 2013).

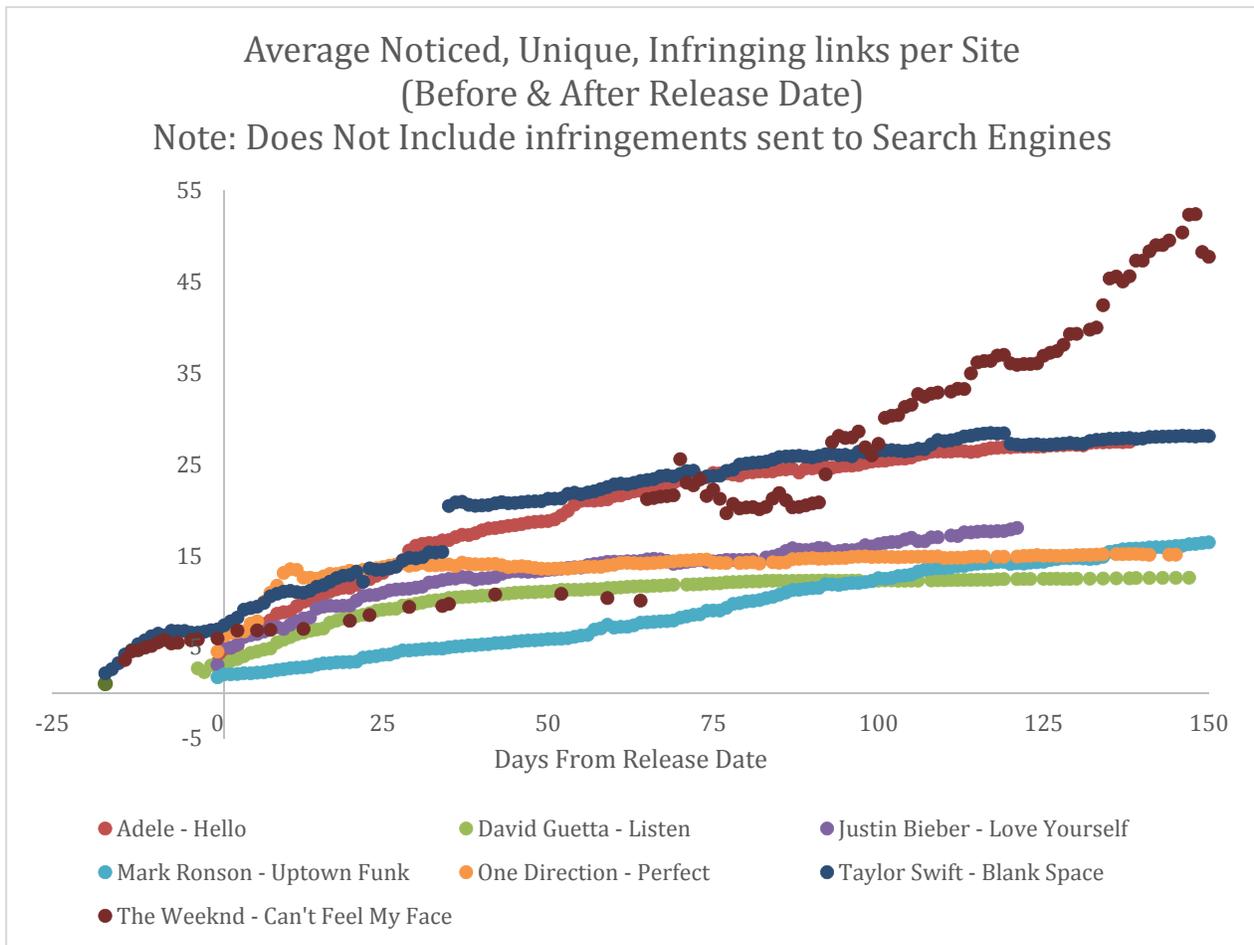
⁵³ This did not include notices for those links to search engines, and includes a period months after the commercial release of these songs.

⁵⁴ See Stephen Witt, *The Man Who Broke the Music Business*, THE NEW YORKER (Apr. 27, 2015), <http://www.newyorker.com/magazine/2015/04/27/the-man-who-broke-the-music-business> (describing some of the history of online infringement of pre-release music); see also Stephen Witt, *How Music Got Free: The End of an Industry, the Turn of the Century, and the Patent Zero of Piracy*, (Viking Pres, 2015); Andre Yoskowitz, *FBI Takes Down Pre-Release Music Piracy Site Share Beast*, NEWS BY AFTERDAWN (Sept. 16, 2015), <http://www.afterdawn.com/news/article.cfm/2015/09/16/fbi-takes-down-pre-release->

infringement is particularly damaging as it hits before the music has been released commercially to the public.

Chart 6.1 illustrates the ratio of infringing links per site noticed around the time of release for several recently released popular sound recordings.

Chart 6.1 – Average Noticed, Unique, Infringing Links per Site (Before & After Release Date)

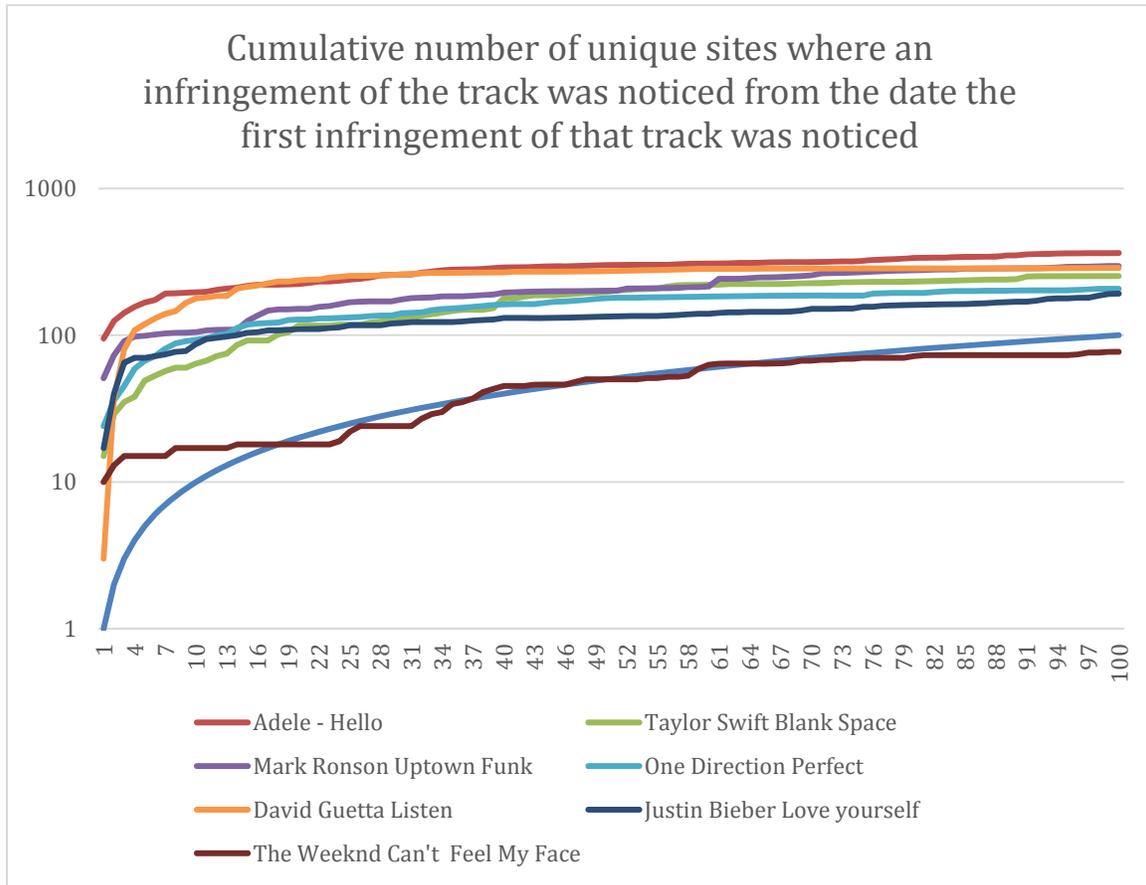


As shown, sometimes serial and viral infringement is found even before the release date of the track. Once the sound recordings were released, the scope of the infringement problem quickly escalated. For example, by the fifth day after commercial release, the number of infringements noticed per site had expanded to over five per site per day.

Chart 6.2 shows how quickly the infringements spread to different sites, based on what could be identified within the limited resources of existing content protection operations.

music-piracy-site-sharebeast (describing ShareBeast, a rogue cyberlocker shut down by the Department of Justice in 2015 that trafficked in pre-release music).

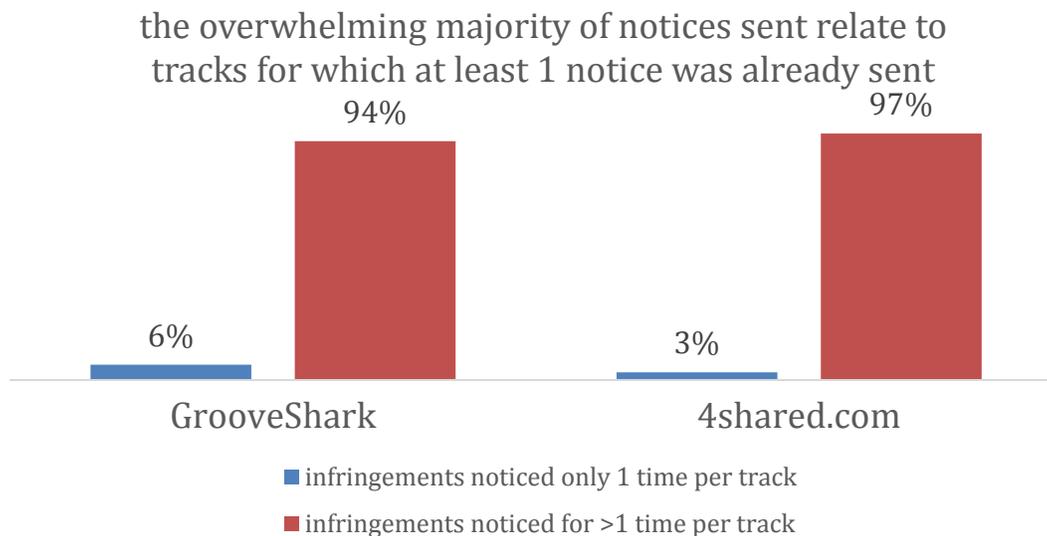
Chart 6.2 – Cumulative number of unique sites where an infringement of the track was noticed from the date of the first infringement of that track was noticed



Unauthorized copies of virtually all these works were found on at least 10 different sites within the first couple of days of release, with several being infringed on over 100 different sites by the end of the first week. This is despite right holder efforts to take down the infringements.

With that understanding of the scope of the problem, consider the ineffectiveness of the DMCA. In 2014, RIAA noticed over 278,000 instances of music infringement to just one site that claims to comply with the DMCA Section 512(c) safe harbors, 4shared.com, a cyberlocker and file sharing hub. Of those, 97% were for repeat infringements of a previously noticed sound recording. In the five months prior to Grooveshark being shut down for willful copyright infringement, RIAA sent the service nearly 300,000 infringement notices; 94% were for repeat infringements of a previously noticed track.

Chart 6.3 – the overwhelming majority of notices sent relate to tracks for which at least 1 notice was already sent



This problem with repeat infringement of the same track on the same site is not limited to a particular class of service provider. IFPI, an international music trade association, reported that infringements of One Direction’s “Drag Me Down” reappeared over 2,700 times on YouTube (an on-demand, audio-visual service) following the first notice, infringements of Mark Ronson’s “Uptown Funk” reappeared over 3,000 times on SoundCloud (an on-demand, music streaming service) following the first notice.⁵⁵

Copyright owners should not be required to engage in the endless game of sending repeat takedown notices to protect their works, simply because another or the same infringement of the initially noticed work appears at a marginally different URL than the first time. The current standard of “URL by URL” takedown does not make sense in a world where there is an infinite supply of URLs. As described in the response to Question 15, technologies exist to identify content that is reposted on a digital service after it is removed, services of all sizes have implemented them, and they should be deployed as a standard industry practice.

We see very similar inefficiencies with search engines, who claim safe harbor status, and the way they continue to index known, infringing sites. Consider the example of the Mp3Skull site, found at various domains in 2015, and the numbers of infringements continually indexed by Google to that infringer. This site jumped to a new domain every time Google demoted the old domain, and that switch to the new domain allowed them to reappear prominently in Google search results.

Chart 6.4 below lists the number of infringing links RIAA noticed to Google for Mp3Skull at some of its various domains through 2015.

⁵⁵ IFPI submission, *supra* n. 34.

Chart 6.4– Infringements Noticed just by RIAA to Google about one rogue service, Mp3Skull, at its various domain addresses⁵⁶

Domain Address for Mp3Skull	# infringements noticed
Mp3skull.com	1,759,947
Mp3skull.to	20,145
Mp3skull.cr	87,971
Mp3skull.is	67,274
Mp3skull.wtf	46,377
Mp3skull.la	70,225
<i>Total</i>	<i>2,051,939</i>

As noted in the response to Question 13, each of these domains pointed to the same underlying IP address,⁵⁷ and continued to redirect to its then current domain address. Despite all of this knowledge about rampant infringement on this rogue service, Google continued to regularly index and point users to it as it hopped domains.

In fact, RIAA provided notices to Google about continued infringements of at least 3,000 tracks on each of these Mp3Skull domains. These tracks included, among others, those set forth in Chart 6.5. Clearly there are inefficiencies at play when Google has received so many notices about the same track at on this service and yet it continued to index infringements for the same track on the same service.

⁵⁶ Most recently, the Mp3Skull site has moved from .la to .yoga, to .mn, and as of March 28, 2016, back to .is.

⁵⁷ As reported by CloudFlare to RIAA.

Chart 6.5 - # of infringements noticed for sample track on Mp3Skull at the domains noted

artist track	mp3skull.com	mp3skull.to	mp3skull.cr	mp3skull.is	mp3skull.wtf	mp3skull.la
big sean blessings	33	31	54	47	17	28
calvin harris under control	269	6	84	25	15	33
fifth harmony worth it	21	26	50	34	16	18
a great big world say something	323	2	67	32	25	11
santana smooth	531	12	47	40	19	6
zedd find you	819	9	46	28	11	27
eiffel 65 blue	341	10	36	18	39	18
calvin harris outside	150	10	32	28	30	19
years years king	18	28	42	22	4	19
ariana grande almost is never enough	227	18	50	29	11	7
schoolboy q studio	416	18	35	37	11	13
august alsina no love	226	15	37	30	16	14
mila j my main	99	7	36	20	37	8
austin mahone mmm yeah	266	15	29	31	16	13
little mix move	360	16	44	27	5	12
jennifer lopez booty	288	6	34	26	9	27

Another major inefficiency in the DMCA, as implemented in today’s environment, is the lack of clarity about what is meant by “expeditious” takedown⁵⁸, and the ability of services to game the system under the veneer of protecting their user base. “Expeditious” takedown must be interpreted to be commensurate with the speed at which infringing material can be uploaded, indexed and disseminated over the Internet.⁵⁹ Google touts that it removes noticed infringing URLs from its system within six hours, but fails to provide transparency about the speed by which it indexes those infringing sites. Six hours on its own is a meaningless statistic in thinking about what “expeditious” means without an understanding of Google’s capabilities and speed in indexing infringing services in the first place. This can be a particularly crucial window of time in the case of works that have not yet been commercially released. Another service recently announced, supposedly for the benefit of its users, that it would institute a 48-hour rule before taking down infringing content that has been the subject of a DMCA notice.⁶⁰ That guarantees for this service, and its users, the ability to continue to benefit from the

⁵⁸ 17 U.S.C. § 512(c)(1)(A)(iii) (“upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material”) and 17 U.S.C. § 512(d)(1)(C) (“upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material”).

⁵⁹ For example, as noted in response to Question 9, last year YouTube CEO Susan Wojcicki announced that over 400 hours of video were being uploaded onto YouTube per minute.

⁶⁰ See *A Fair DMCA Policy for Creators*, PATREONBLOG (Feb. 22, 2016), <http://blog.patreon.com/a-fair-dmca-policy-for-creators/>.

infringement during this period. If a service wants to institute such a policy to keep the alleged infringement up after notice for whatever reason, that is a business risk it can take, but it should not be permitted to continue to avail itself of the safe harbors for any activity on its service. The law must be clarified to reflect this.

For further inefficiencies in the DMCA process, please see responses to Questions 16 and 26 on the issues surrounding the current abuse of the counter-notice procedure by users.

In thinking about the problem of repeat infringements, prominent scholars have advocated that recalibration is necessary, and suggested that a return to more traditional tort principles would help solve this concern.⁶¹ This proposal should be seriously considered.

7. How efficient or burdensome is Section 512's notice-and-takedown process for addressing online infringement? Is it a workable solution over the long run?

Section 512's notice-and-takedown system is unduly inefficient and burdensome for a number of reasons, including the whack-a-mole nature of the problem and the lack of a serious "takedown-and-staydown" component, both discussed in response to Question 6, above.

As a general matter, the DMCA, as currently interpreted by some service providers, requires content owners to survey every link on the Internet, worldwide, twenty-four hours a day, seven days a week, three hundred and sixty-five days a year, while service providers take advantage of the DMCA to profit from the infringing activity. Even with large-scale content owners with a large back office and significant resources, these efforts are only minimally effective. Smaller copyright owners – like songwriters, indie artists, indie labels and publishers – cannot even engage in these minimally effective efforts and have no remedy at all.

As noted above, RIAA alone has sent notices of over 175 million infringements. And the music industry regularly has to send notices of repeat infringements of the same copyrighted content to or about the same digital services over and over again. In just the first two months of 2016, RIAA sent repeat notices of infringements on over 6,500 tracks to just one service claiming DMCA safe harbors.⁶²

The process has gotten so out of hand that at least one service provider that claims safe harbor protection has told RIAA that receiving a notice about one link to an infringing file it hosts will not lead to a takedown of any other links it provides to exactly the same file. That service provider reasons that while it can condense user uploads of

⁶¹ See Peter S. Menell and David Nimmer, *Legal Realism in Action: Indirect Copyright Liability's Continuing Tort Framework and Sony's DeFacto Demise*, 55 UCLA L. Rev. 1 (2007). See also Bruce Boyden, *The Failure of the DMCA Notice and Takedown System*, CENTER FOR THE PROTECTION OF INTELLECTUAL PROPERTY (Dec. 2013), available at <http://cpip.gmu.edu/wp-content/uploads/2013/08/Bruce-Boyden-The-Failure-of-the-DMCA-Notice-and-Takedown-System1.pdf> for a discussion of other solutions to address the repeat infringement problem.

⁶² Source: RIAA (based on notices sent for 4shared.com).

the same content into one file so that it can conserve server space, it is inappropriate for the site to be obligated to remove all links its service created to that file upon a DMCA notice that specifies only one of those links, because the other uploaders might have authorization to upload that file. This is contrary to the express provisions of the DMCA.

If the current trend continues, the burden will only become worse. Digital use of copyrighted content is increasing. Congress must take this into consideration as it looks at reforming the notice-and-takedown process. Implementing a system where a notice sent to a service provider will be valid beyond the initial identification of an infringement, and strengthening the use of “representative lists” of content provided to intermediaries, will go far in relieving the burden placed on the copyright owner under the present DMCA system.

8. In what ways does the process work differently for individuals, small-scale entities, and/or large scale entities that are sending and/or receiving takedown notices?

As noted throughout our comments, the notice-and-takedown system is challenging, cumbersome, and expensive for all copyright owners. Even for large entities it is a serious resource challenge. But for small-scale entities and individual creators, the challenge is almost impossible to meet. The process is so daunting that many have stopped sending takedown notices altogether, and some conclude that they literally have no remedy under the DMCA, and no real way to protect the value of their works from indiscriminate infringement.

For example, Maria Schneider, a three-time GRAMMY winning jazz and classical composer, bandleader and conductor, notes that her most recent album has been available, for free and without her authorization, on numerous file sharing websites, and proposes that in the case of unauthorized verbatim copies, which cannot possibly be fair use, content matching technologies should be used to *prevent* infringement *before* it occurs, rather than solely to identify infringement after it occurs.⁶³

Musician Eric Hilton, founder of ESL Music and Thievery Corporation, believes that even with the existence of viable content ID and filtering systems, the greatest challenge is to require the companies to use the technology. Most of these companies are conditioned and dedicated to ignoring the existence of the problem – essentially engaging in a form of willful blindness. Quite simply, without a strong legal deterrent mandating the use of such systems, service providers and other intermediaries will never engage in the effort. It is in their best interest for the status quo to continue.⁶⁴

⁶³ See House Judiciary Subcommittee Section 512 Hearing, 113th Cong. 57 (2014) (statement of Maria Schneider).

⁶⁴ See ESL Music Letter, Appendix E.

“This view is shared by small independent record labels. Notice-and-takedown is simply not a viable remedy for the rest of the world. Only a viable ‘notice-and-staydown’ program will work for copyright owners, particularly the smaller entities.”⁶⁵

9. Please address the role of both “human” and automated notice-and-takedown processes under Section 512, including their respective feasibility, benefits, and limitations.

In today’s environment, a combination of automated and human takedown processes are required to deal with user-uploaded and automated, un-curated, unscreened upload/indexing processes. Last July, YouTube CEO Susan Wojcicki announced that over 400 hours of video were being uploaded onto YouTube every minute.⁶⁶ That translates into over 1,000 days’ worth of content per hour, for just a single user-uploaded content service. The Music Community would be severely handicapped without the ability to use automated tools to match this unprecedented scale of uploading of content.

A thoughtful implementation of a combination of automated and human infringement identification and notice processes is often quite accurate. For example, RIAA’s procedures and infringement identification track record, based on automated and human processes, has been viewed as good by service providers.⁶⁷ Conversely, a human only process to identifying infringements and sending notices is clearly ineffective in today’s environment.⁶⁸ However diligent a creator or owner may be in trying to protect a single work, sufficient person-hours will never be available to them to deal with the scale of uploading that exists today.⁶⁹

At the end of the day, if service providers are permitted and encouraged to automatically post thousands of pieces of user-uploaded content without requirement to conduct any level of analysis whatsoever as to whether that content is likely to infringe a third party’s rights, then rights holders must have commensurate tools to address that infringement.

10. Does the notice-and-takedown process sufficiently address the reappearance of infringing material previously removed by a service provider in response to a notice? If not, what should be done to address this concern?

The notice-and-takedown process, as currently implemented by some providers, does not in any manner address the reappearance of infringing material previously removed by a provider in response to a notice. Please see the responses to Questions 6 and 7 above and Question 13 below, for various examples of the repeat infringement problem across various classes of digital services.

⁶⁵ A2IM.

⁶⁶ Mark R. Robertson, *500 Hours of Video Uploaded to YouTube Every Minute [Forecast]*, REELSE (Nov. 13, 2015), <http://www.reelseo.com/hours-minute-uploaded-youtube/>.

⁶⁷ For example, RIAA is part of Google’s trusted notice sender program.

⁶⁸ See the individual submissions by Universal Music Group, Warner Music Group and Sony Music.

⁶⁹ Please see response to Question 8 for some of the experiences owners and creators have had with using a human only review process.

In some cases, the repeat infringement is of the same file previously noted as being infringing. In other cases, it can be a repeat infringement of the same full length sound recording previously noticed, but may involve a file with a different hash. In yet other cases, the repeat infringements may involve variations of infringements of the previously noticed copyrighted work. In all these cases, even though the copyright owner has noticed the service that it has not authorized the use of its work on that service, the service permits further infringements of the copyrighted work to continue until the specific URL where that instance is located is identified in a DMCA notice.

As discussed in responses to Questions 14 and 19, this problem is exacerbated by judicial interpretations of “representative list” and “red flag” knowledge. These judicial interpretations embolden some service providers to take little or no action to address further infringements of the same copyrighted work on their service, if only one or a sample of fewer than all URLs for the infringements of that copyrighted work are noticed to the service.

This is simply not a system that Congress designed or ever would have designed. The statute must be revised to stop service providers and their users from gaming the system in this way.

11. Are there technologies or processes that would improve the efficiency and/or effectiveness of the notice-and-takedown process?

Technologies and processes exist today, and others can be readily adapted, to improve the efficacy of the notice-and-takedown process, at least with respect to sound recordings. These include, among others:

- Audio fingerprinting technologies to prohibit the redistribution or posting of unauthorized sound recordings that match previously noticed copyrighted sound recordings or musical works.
- Hash-matching technologies to prohibit the redistribution or posting of the exact instances of infringement previously noticed as infringing.
- Meta-data correlations by a service provider to identify potential infringements of previously noticed copyrighted works.
- Automatic removal and/or disabling of any links that point to a previously noticed infringement.

While several of these technologies and processes have challenges and limitations, they at least represent an improvement over the status quo. And several digital services, both large and small, use such technologies today.⁷⁰ Please see the

⁷⁰ See, e.g., *How Content ID Works*, YOUTUBE HELP, <https://support.google.com/youtube/answer/2797370?hl=en>, last accessed March 29, 2016; *An Update on Video Management on Facebook*, FACEBOOK MEDIA (Aug. 27, 2015), <http://media.fb.com/2015/08/27/an-update-on-video-management-on-facebook/>; *Customer Partners*, AUDIBLE MAGIC,

response to Question 15 for a further discussion of such technologies, and the impact they have had on the problem of repeat infringements.

Google often suggests that it cannot practically address the fact that it continuously indexes unauthorized copyrighted works on third party sites. It claims this even though it has received numerous notices of infringements of the same copyrighted work on the same third party site, even in cases where the new URL is only slightly changed (*e.g.*, www.roguesite.infringeadelehello-1 to www.roguesite.infringeadelehello-2), and even though Google apparently knows enough about the revised URL to serve it in the first page of search results when looking for a sound recording of the previously noticed track. If Google can develop programs to play and beat a master of the complex game Go,⁷¹ it can certainly develop programs to address this repeat infringement problem in its indexing function.

Some opponents of adopting technological processes to detect and deal with infringing content argue that content matching systems would result in an increase in false notices, and consequently, could disproportionately impose on user's free speech and expression rights. The data show that those claims are overblown and not consistent with the facts. For example, YouTube employs content identification technology. Nonetheless, as noted in responses to Questions 16 and 26, in one month, one music trade association noticed 98,753 infringements of sound recordings to YouTube. Only 653 counter-notices were filed on those notices by users claiming that the notices were improperly sent. Even assuming that free speech concerns underlay every one of these counter-notices, and even assuming all of them were valid, this is very thin evidence of disproportionate impact.⁷²

In addition, as discussed in response to Question 9, there are automated tools that can be and have been implemented thoughtfully by rights holders to scan for and identify

<http://audiblemagic.com>, *last accessed* March 29, 2016 (a list of companies using its audio fingerprinting solutions, which includes AOL, Facebook, MySpace, SoundCloud, Veoh and Vimeo, among others); Cloud Fender, *What happens when you share copyrighted stuff on DropBox*, MEDIUM (Nov. 19, 2014), <https://medium.com/productivity-in-the-cloud/what-happens-when-you-share-copyrighted-stuff-on-dropbox-5e7e0f44b3df#.nt5px8haj>; *see also* *What We Do*, VOBILE, <https://www.vobileinc.com/about>, *last accessed* March 29, 2016 (commercial solutions to protect audio-visual works).

⁷¹ Choe Sang-Hun and John Markoff, *Master of Go Board Game Is Walloped by Google Computer Program*, NEW YORK TIMES (March 9, 2016), <http://www.nytimes.com/2016/03/10/world/asia/google-alphago-lee-se-dol.html>.

⁷² When YouTube wants to ensure content is not available on its free service, it certainly knows how to effectively make that happen. For example, Indie artist Zoe Keating was told her content channel would be "blocked" if she did not sign YouTube's licensing agreement as it was presented. Furthermore, whether she signed or not, content uploaded by users would be added to YouTube's Music Key, regardless of whether she had authorized any such distribution of her content. Glenn Peoples, *Cellist Zoe Keating Opens Up on Her YouTube Battle: 'There's a Lot of Fear Out There'*, BILLBOARD (Jan. 28, 2015), <http://www.billboard.com/articles/business/6451152/qa-zoe-keating-youtube-battle-theres-a-lot-of-fear>. YouTube has also announced that YouTube is launching a new subscription service, YouTube Red, with exclusive and original content available ad-free and at no extra charge only to paying subscribers. Todd Spangler, *YouTube Set to Premier First Original Movies, PewDiePie Series*, VARIETY (Feb. 3, 2016), <http://variety.com/2016/digital/news/youtube-first-original-movies-pewdiepie-show-1201695813/>. It will be interesting to watch what efforts YouTube takes to ensure that content doesn't show up on its free service, and how those efforts compare to its efforts to deter infringements of third party content.

infringements, that are then sent to digital services for remedial action. Such automated tools help speed up the identification of infringing links, and, as noted above, can also improve the accuracy of such infringement identification. However, improving the efficiency of finding infringements and sending notices about them does not solve the underlying problem of repeat infringements, and the rapid proliferation of infringing works in the digital marketplace.

12. Does the notice-and-takedown process sufficiently protect against fraudulent, abusive, or unfounded notices? If not, what should be done to address this concern?

The protections that exist today not only protect against unfounded notices, but, as noted in responses to Questions 16-18 and 26, they can go too far in trying to protect the uploader and service provider. Section 512(c)(3) provides many necessary elements for an effective takedown notification, including a statement “that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.” While everyone makes honest mistakes, the liability provided by Section 512(f) is a significant deterrent. Consider, as noted in responses to Questions 11, 18 and 26, on a sample of 98,753 infringements noticed to one site, only 0.7% received a counter-notice. However, of those counter-notices, over 80% seemed likely to be unfounded. While certainly there are anecdotes of fraudulent notices, as the data show, they are very few and far between.⁷³ Further changes to the DMCA to protect against fraudulent notices are unwarranted.

13. Has Section 512(d), which addresses “information location tools” been a useful mechanism to address infringement that occurs as a result of a service provider’s referring or linking to infringing content? If not, what should be done to address this concern?

Given the prominent role “information location tools” have taken on in today’s environment, Section 512(d) has been largely ineffective in addressing online infringement. A recent study shows that search engines are the number one source by which consumers find ways to acquire music for free from unlicensed sources.⁷⁴ Huge volumes of DMCA notices sent to leading search engines have not altered this basic fact.

Search engines take the position that once they are notified that copyrighted content on a particular digital service is infringing, they will remove only the particular URL identified, disregarding the ease with which an infringing service can and will create a new URL to the very same content that is the subject of the takedown notice. That new URL is then re-indexed by the search engine. In 2013, RIAA reported that it

⁷³ Of the retractions submitted by the trade association after reviewing the counter-notices (which accounted for 0.1% of the infringements noticed), we note that the overwhelming majority of them concerned express authorizations granted to use the copyrighted material, and not mistake in identifying the material or other defenses offered by the uploader.

⁷⁴ MusicWatch, *The Environment Around Unsanctioned Music Acquisition* (January 2016). Another study from Carnegie Mellon University, perhaps the most comprehensive study yet on the link between search engines and media piracy, confirmed what search engines have likely known all along: that more highly placed links do have an effect influencing consumer behavior. The study showed that even users looking for lawful content could be led astray by promoted links to pirated content. Sivan, *supra* n. 33.

sent notices to Google of repeat infringements of the same track on 4shared.com at a rate of 1.1 infringements per week.⁷⁵ For the same period in 2015, RIAA continued to have to send Google repeat notices about the same track on the same site. For example, 62% of the infringements noticed to Google during this period occurring on 4shared.com were for repeat infringements of the same track.⁷⁶ The trend was even worse for sites such as the Mp3skull.com family of sites. In 2012, RIAA was sending on average 4.4 notices per week per track to Google about infringements of popular tracks on Mp3skull.com. In the fall of 2015, RIAA sent a similar number of repeat notices per week per track for popular tracks to the then current address for Mp3Skull, Mp3skull.wtf.⁷⁷

In a world of an infinite supply of URLs and sophisticated search engines that can quickly index and categorize these URLs for search purposes, copyright owners should not be required to engage in the constant game of sending repeat takedown notices to search engines for the same sound recording on the same service simply because it appears at a slightly different URL than it originally did. The fact that Google receives and responds to large numbers of notices is not a reflection of the system working, but rather a symptom of the gross inefficiencies of the DMCA. Again, Google should develop programs to address this repeat infringement problem in its search index function.

Google argues that de-indexing an entire site, even though Google has received actual knowledge of millions of infringements on that site, would be “censorship”. It is unclear whose speech Google believes is being censored, but, in any event, when considering the First Amendment and intellectual property rights, a thoughtful weighing and balancing of the interests is required. At some point, when the evidence of infringement on a service is so rampant, and evidence of legitimate speech on the service is minimal, such speech should not benefit from heightened protection. The appropriate remedy in this case is to remove the site from the search engine index.

14. Have courts properly interpreted the meaning of “representative list” under Section 512(c)(3)(A)(ii)? If not, what should be done to address this concern?

Courts have not properly interpreted the meaning of “representative list” under Section 512(c)(3)(A)(ii).

The statute expressly allows copyright owners who learn of the presence of infringing material on a website to notify the service provider of a “representative list” of infringed works thereby requiring the service provider to remove not only the specific works set forth in the notice, but also other clearly infringing material that is not specified in the notice.⁷⁸ The statute specifically considered that this would apply to entire

⁷⁵ *Six Months Later – A Report Card on Google’s Demotion of Pirate Sites*, RIAA (Feb. 21, 2013), available at http://www.riaa.com/wp-content/uploads/2015/10/Google_ReportCard.pdf.

⁷⁶ Source: RIAA

⁷⁷ Source: RIAA

⁷⁸ 17 U.S.C. § 512(c)(3)(A)(ii) (“if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site”).

websites, not specific webpages.⁷⁹ As noted in one of the earlier cases interpreting the DMCA, the purpose of the representative list is to “reduce the burden of holders of multiple copyrights who face extensive infringement of their works.”⁸⁰ In that case, the court denied the defendant’s motion for summary judgment on the grounds that the notice was insufficient.⁸¹ In another early case, the court found that defendant’s policy requiring notices to contain the exact webpage of the infringing material was contrary to the DMCA.⁸²

However, subsequent court interpretations have effectively nullified the representative list provision by either finding such lists insufficient or, notwithstanding the plain language of the statute, requiring a specific URL for each instance of infringement, thus eviscerating the practical effect of a representative list.

- In *UMG Recordings v. Veoh*,⁸³ the district judge, and later the appellate judge, concluded that the DMCA’s liability limitations applied notwithstanding uncontroverted evidence that the service had been informed that any videos on Veoh by a list of recording artists were infringing, that the CEO had admitted knowledge of infringing material service, and other evidence of apparent infringement.
- In *Capitol Records, Inc. v. MP3Tunes, LLC*,⁸⁴ the court found that the representative list provided was insufficient because it did not include specific URLs for all of the locations, noting that while service providers must take down specific material identified in the notice, they are not required to search for or take down other material that may infringe the identified copyrighted work.
- And in *Viacom v. YouTube*,⁸⁵ the court ruled that there must be a specific URL address identified for each instance of an identified infringing work, essentially leaving the representative list provision devoid of any meaning. The court also misconstrued Section 512(m) to require no reactive action by a service provider regardless of the information provided to it about infringing activity via a representative list.⁸⁶

⁷⁹ *Id.*

⁸⁰ *ALS Scan*, 239 F.3d at 625.

⁸¹ *Id.*

⁸² *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

⁸³ *UMG II*, 665 F. Supp. 2d 1099; *aff’d UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022 (9th Cir. 2011) (“*UMG III*”); *UMG IV*, 718 F.3d at 1014.

⁸⁴ 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

⁸⁵ *Viacom*, 718 F. Supp. 2d 514.

⁸⁶ See also Jeremy A. Schachter, *Note and Recent Development: Substantially Perfect: The Southern District of New York’s Problematic Rewrite of the DMCA’s Elements of Notification*, 29 *Cardozo Arts & Ent. LJ* 495 (2011) (criticizing case law on the representative list provision); Philip Mazoki, *CASE NOTE AND COMMENT: Viacom International Inc. v. YouTube Inc. and the Failings of the Southern District Court of New York*, 30 *Temp. J. Sci. Tech. & Env’tl. L.* 275 (2011); Lior Katz, *Note & Comment: Viacom v.*

The scope of infringements in today’s environment makes the “representative lists” provision of DMCA more necessary than ever. As the statute is reformed, the term should be more clearly defined to allow copyright owners to use this and other more technologically feasible methods to put services on notice of widespread and actionable infringement.

15. Please describe, and assess the effectiveness or ineffectiveness of, voluntary measures and best practices – including financial measures, content “filtering” and takedown procedures – that have been undertaken by interested parties to supplement or improve the efficacy of Section 512’s notice-and-takedown process.

Voluntary measures are a useful tool to address infringement when both parties are willing to take practical steps to address the problem. They do not, however, represent a silver bullet that solves the inequities that exist in today’s digital environment. To work effectively, voluntary measures must take place against the backdrop of practical, effective, and balanced laws that create an environment where all stakeholders see value in pursuing such measures. The DMCA, as currently interpreted, does not encourage this approach.

Currently, the interests of content and some tech companies do not often align on certain aspects surrounding the DMCA and a notice-and-takedown regime. Consider, for example, the recent exercise on notice-and-takedown best practices facilitated by the Commerce department.⁸⁷ Rights holders, individual creators, service providers of different sizes, and consumer and public interest representatives, including several representatives from the Music Community, participated in this process. Meetings took place every six weeks through the end of the year, but the result, while useful, only addressed limited efficiencies in the DMCA, despite calls for discussions to address efforts to increase the effectiveness of the notice-and-takedown regime. The misalignment of interests prevented such discussions from meaningfully taking place. This lack of cohesion and misalignment of present interests underscore the need for legislative reform in defining and establishing standard technical measures (“STMs”).

For a detailed description of various voluntary measures that have been considered and the challenges faced with effectively negotiating and implementing them, please see the October 2015 comments to the Intellectual Property Enforcement Coordinator, attached hereto as Appendix C.⁸⁸

To supplement those comments, we note the following additional observations.

YouTube: An Erroneous Ruling Based on the Outmoded DMCA, 31 Loy. L.A. Ent. L. Rev. 101 (2010-11); and 4 Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* § 12B.04.

⁸⁷ Department of Commerce, *DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices*, DMCA MULTISTAKEHOLDER FORUM, available at http://www.uspto.gov/sites/default/files/documents/DMCA_Good_Bad_and_Situational_Practices_Document-FINAL.pdf, last accessed March 29, 2016.

⁸⁸ See also RIAA Comments, USPTO’s Request for Comments in its Voluntary Best Practices Study (Aug. 19, 2013), <http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf#page=15>.

Financial Measures. In the past few years, there has been a more concerted effort on the part of payment processors, ad networks, and advertisers to stop the flow of funds from these intermediaries to services engaged in rampant widespread copyright infringement. We believe these measures have made a positive impact in that they have limited the sources of funding for these infringing services and also caused the sites to look illegitimate, discouraging some visitors. For example, in the summer of 2015, a major payment processor stopped providing payment services to a rogue infringing cyberlocker, and in response, at least one of the cyberlocker's uploaders claimed it would no longer source third party content to the cyberlocker because it could no longer receive payment from that cyberlocker.⁸⁹ Also, on February 11, 2016, the Trustworthy Accountability Group ("TAG", at tagtoday.net) announced it was moving its program to deter the flow of advertising dollars to criminals engaged in piracy from the design phase to the execution phase. We look forward to seeing how this program progresses.

Content Matching Technologies. While there is no multi-industry initiative on the use of content matching technologies, several digital services, including YouTube, Tumblr, SoundCloud, 4shared, and others, have unilaterally implemented some form of content matching and have taken action based on that matching to deter further infringement. Content matching solutions include proprietary systems, hash-based file identification, and/or various implementations of third party fingerprinting solutions, such as Audible Magic.

The type of technology used and its implementation significantly affect the scope of the content identified, the action taken after such content is identified, and its overall effectiveness. For example, for a service that implemented hash-based content identification, the number of notices of repeat infringement that were sent by RIAA declined only slightly, from 99% repeat infringements to 97% the following year. On the other hand, when a service used a more robust Audible Magic implementation designed to address master sound recordings, RIAA found that, after such implementation, no meaningful infringements of full commercially released sound recordings were hosted on that service. This meant RIAA could focus its efforts on this service to detecting and dealing with on pre-release leaks, for which content matching was not yet available.⁹⁰

⁸⁹ See comments by user tomlav2634 left on discussion on wjunction.com, visited on July 20, 2015.

⁹⁰ We also note that while courts have not gone so far as requiring service providers to utilize content identification technologies to prevent infringement, one case found that LiveJournal's "anti-spam" system, which it employed voluntarily to block posts with keywords related to notices it had receive, would be a type of "technological measure" that could be required by an injunction issued under § 512(j)(1)(A)(iii). See *Mavrix Photographs LLC v. LiveJournal, Inc.*, No. SACV 13-00517-CJC(JPRx), 2014 U.S. Dist. LEXIS 160324, *27-28 (C.D. Cal. Sept. 19, 2014). For services where infringement is occurring on a large scale, forward-looking injunctions requiring screening of uploads based on artists' names and titles, for example, would shift the burden to services to screen, review, and then post harmless content. Many sharing sites, like YouTube and Facebook, already employ large back offices offshore for screening for offensive content. See, e.g., Adrian Chen, *The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed*, WIRED (Oct. 23, 2014), <http://www.wired.com/2014/10/content-moderation/>; and Adrian Chen, *Inside Facebook's Outsourced Anti-Porn and Gore Brigade, Where 'Camel Toes' are More Offensive Than 'Crushed Heads'*, GAWKER (Feb. 16, 2012), <http://gawker.com/5885714/inside-facebooks-outsourced-anti-porn-and-gore-brigade-where-camel-toes->

The implementation of such technology is certainly appreciated by the Music Community but should not be seen as a panacea, particularly when, despite the availability and increased use of content matching technologies, to date services have been unwilling to address these issues on an industry-wide basis.

Search Engine Demotion. In October, 2014, Google introduced an enhanced “demotion” signal to deprioritize sites for which it had received high numbers of notices. However, Google has provided no transparency into how this demotion signal works in practice. Worse, it appears that Google does not take into account previous notices sent about a service when it merely “hops” to a different domain. This apparently allows an infringing service to wipe the slate clean and avoid demotion simply because it changed the location of its domain on the Internet.

As demonstrated in the following charts, while Google’s demotion signal appears to impact traffic to a particular domain, the clock apparently starts over if the service merely switches its domain address. Chart 15.1 shows the number of infringements noticed to Google (from all sources) about Mp3Skull at its various domain locations in 2015. Chart 15.2 shows the frequency with which the various Mp3Skull domains appeared in the top 10 search results for searches for the top 50 Billboard tracks. Each of these domains at some point in 2015 included a “301 redirect” to automatically direct visitors to the subsequent domain, and each of these domains points to the same underlying IP address for the site. In essence, the service hasn’t changed its true address or underlying function – it merely changed the pointer to it. Nonetheless, even though Google had received notices of over 500,000 infringements on Mp3skull.to and demoted that domain, upon redirection of the service to Mp3skull.cr, Mp3skull.cr immediately gained popularity in search results. And the same trend continued as Mp3Skull hopped to various other domains.

are-more-offensive-than-crushed-heads. Therefore, these companies already have the workforce and infrastructure for screening and blocking.

Chart 15.1 – Infringements Noticed To Google about Mp3Skull⁹¹

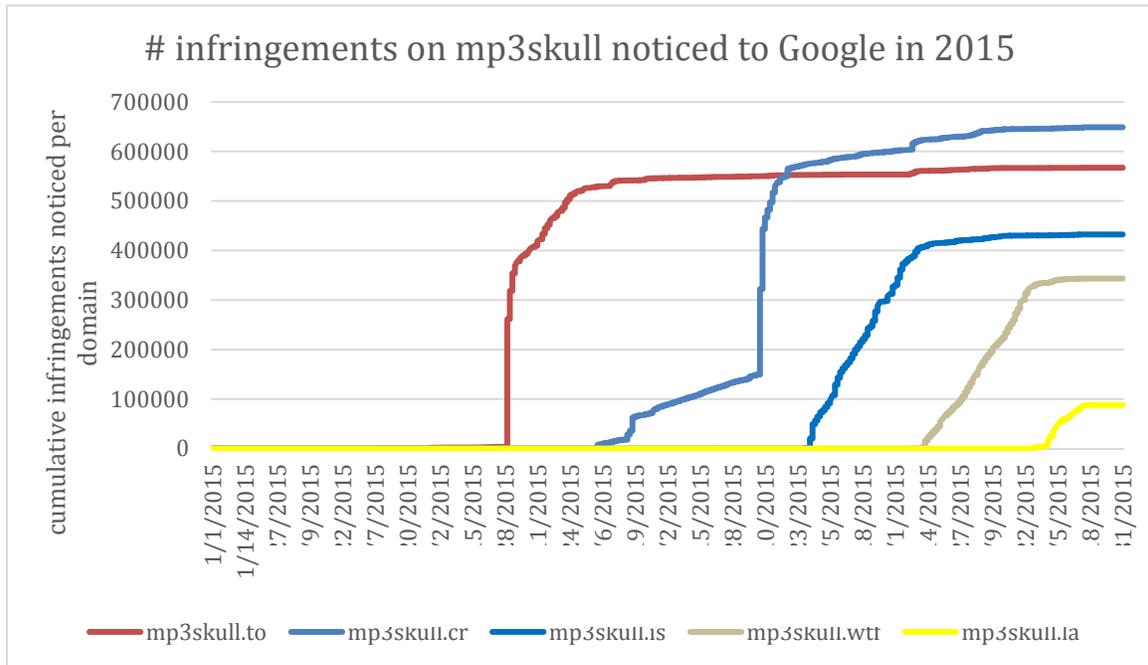
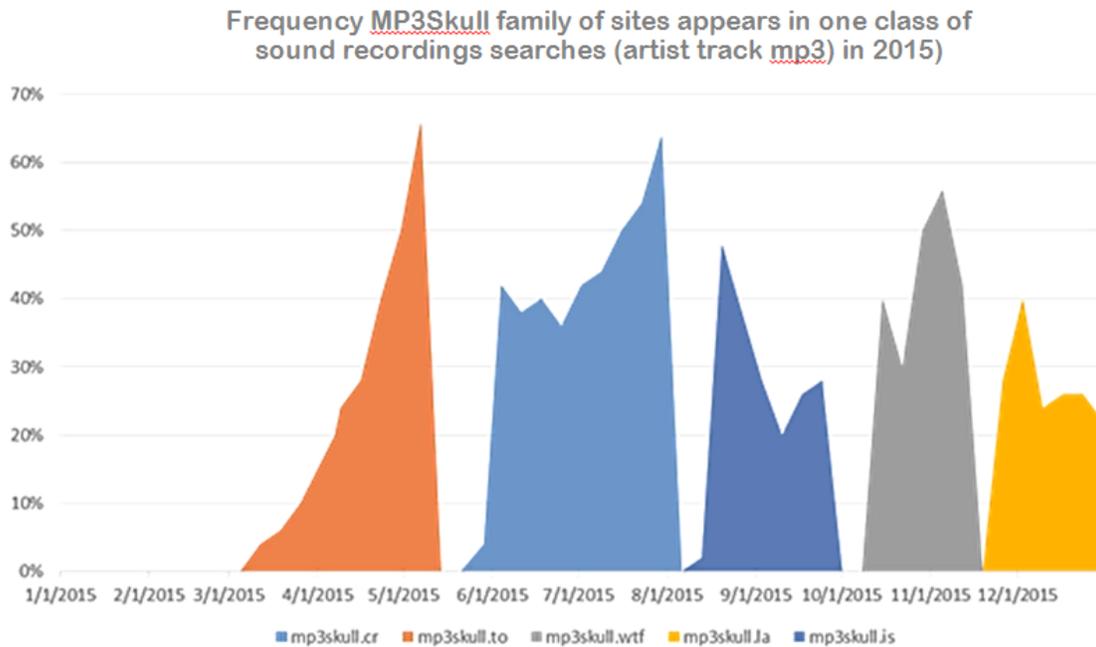


Chart 15.2 – Frequency Mp3Skull family of domains appears in one class of sound recording searches in 2015⁹²

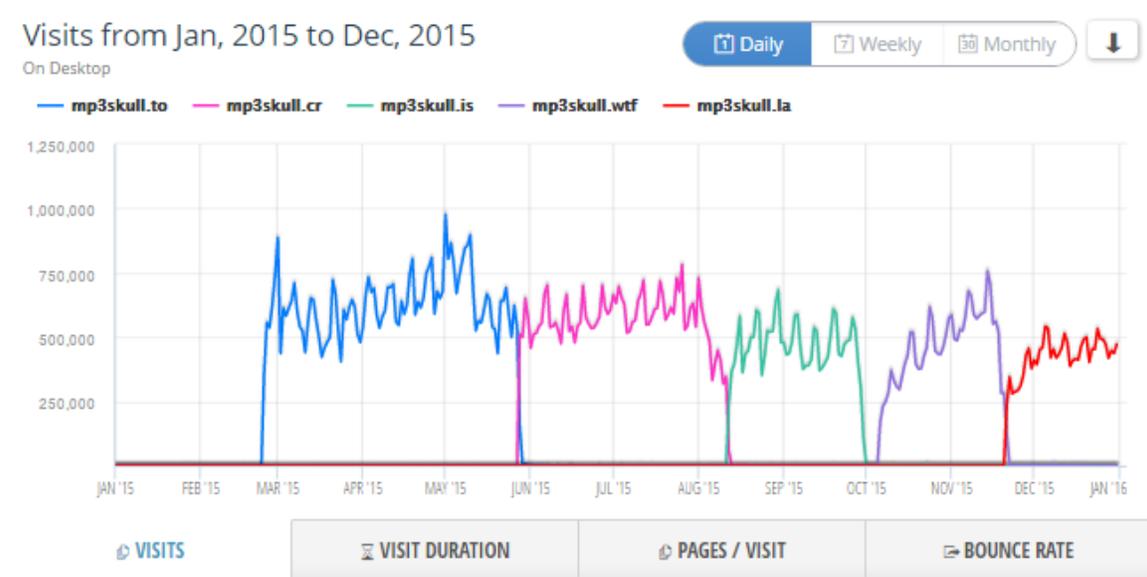


⁹¹ Source: RIAA analysis. This excludes the millions of infringements previously noticed to Google about Mp3skull.com.

⁹² Source: RIAA analysis.

As shown in Chart 15.3, this situation resulted in Mp3Skull not suffering any significant decrease in traffic for 2015.⁹³

Chart 15.3 – Traffic to Mp3Skull family of domains⁹⁴

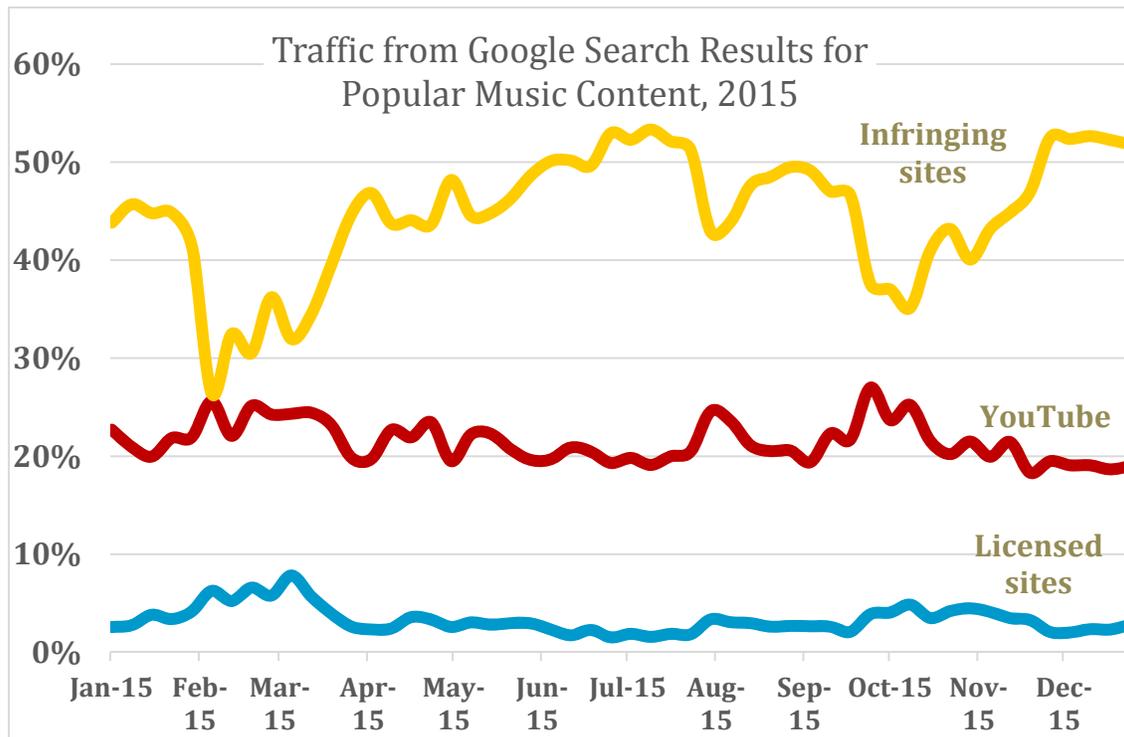


More importantly, while the demotion signal impacts traffic to a particular domain, it does not negatively impact the overall trend of infringing services promoted in Google search results for searches for popular music. In fact, as shown in Chart 15.4 below, estimated traffic to infringing services from Google search results for popular music in 2015 continued to rise, while traffic to licensed services and to YouTube remained flat.

⁹³ Per Similarweb, in January 2016, Mp3Skull received over 50% of its traffic from search, and over 75% of that from Google.

⁹⁴ Source: Similarweb.

Chart 15.4 – Traffic from Google Search Results for Popular Music Content 2015⁹⁵



In sum, search engines continue to provide a critical link between digital services that infringe copyrights and the audiences they seek to serve, including U.S. consumers. While demotion efforts have made some difference, without greater cooperation by the major search engines, pirate services will continue to benefit from the substantial traffic sent to them by search engines. Unfortunately, efforts to encourage these critical players in the e-commerce environment to work cooperatively toward a sensible framework for this problem have failed to gain traction. Notices to search engines about repeat infringement on the same service need to have a meaningful impact, or there must be a tipping point where whole site removal from the search engine index is warranted.

Accordingly, while voluntary measures should be encouraged and services should be incentivized to implement them, the effect of such measures will not be adequate to combat copyright infringement, as long as such voluntary measures exist in a legal environment that does not more closely align the interests of service providers and rights holders.

⁹⁵ Source: IFPI Analysis. This is based on estimated traffic from weekly search results for searches for the then current top 50 Billboard tracks and mp3s and downloads of those tracks. For purposes of this analysis, an infringing site is one where the majority of the content on the homepage of the site infringes copyright (or, if the homepage has no content like TPB or Kickass, then a general assessment of the site indicates that the majority of the content available infringes copyright), and licensed sites are those listed on the Pro Music site, <http://pro-music.org/>.

V. COUNTER-NOTIFICATIONS

16. How effective is the counter-notification process for addressing false and mistaken assertions of infringement?

In our experience, the counter-notification process results in too many false-positive counter-notices. For example, IFPI received counter-notices on 653 infringements, based on a sample of 98,753 infringements noticed to YouTube.⁹⁶ After reviewing these counter-notices, it appeared that over 80% of the counter-notices had no good faith basis for claiming “mistake or misidentification,” the only valid statutory grounds for a counter-notification⁹⁷ Yet, based on this sample, the association representing the rights holders would be required to institute over 500 lawsuits in order to enforce their rights.⁹⁸ This is an unmanageable burden. These statistics further demonstrate that the deck is unfairly stacked against rights holders. Unfortunately, uploaders of third party content are often either misinformed or encouraged to file counter-notices without a basic understanding of their rights and obligations concerning their use of third party content.⁹⁹

Clearly, the system needs to be rebalanced or reconsidered in its entirety.

17. How efficient or burdensome is the counter-notification process for users and service providers? Is it a workable solution over the long run?

Further to the response to Question 16 above, it appears to us that the counter-notice process is much too easy for uploaders, and results in far too many counter-notices that lack any good faith belief of mistake or misidentification. This is not a workable solution over the long run because it leads to misconceptions about the law, and copyright owners must either engage in expensive litigation or have no recourse. In practice, there is no meaningful difference between a proper counter-notification and a legally sanctioned “putback” of material, even if clearly infringing.

18. In what way does the process work differently for individuals, small-scale entities, and/or large scale entities that are sending and/or receiving counter notifications?

For rights holders, whether small or large, properly addressing counter-notices in today’s environment is an insurmountable task. As noted above, uploaders are encouraged to file counter-notices often without understanding their rights and obligations. Further, there is a mounting perception that there is no financial risk or other down-side to filing counter-notices. This results in significant numbers of counter-notices that are false, leaving copyright holders with the significant burden of either filing

⁹⁶ Source: IFPI.

⁹⁷ Source: IFPI analysis. See 17 U.S.C. § 512 (i)(1)(A).

⁹⁸ See also the individual submissions by Universal Music Group, Warner Music Group and Sony Music on their experiences with the counter-notice system.

⁹⁹ See *DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices*, supra n. 87; see also, e.g., “What Is Fair Use?”, YOUTUBE, <https://www.youtube.com/yt/copyright/fair-use.html>, last accessed March 29, 2016.

expensive and lengthy litigation in a very short time frame, or being left with no remedy at all.

Most artists simply do not have the resources to engage in such a costly, and time compressed litigation. Don Henley is the only artist we know of to date who has actually sued under the counter-notification provision.¹⁰⁰ Clearly the cost of such a lawsuit, and the short turnaround time, has effectively pre-empted other artists with fewer resources from engaging in such an exercise.

VI. LEGAL STANDARDS

19. Assess courts' interpretations of the "actual" and "red flag" knowledge standards under the Section 512 safe harbors, including the role of "willful blindness" and Section 512(m)(1) (limiting the duty of a service provider to monitor for infringing activity) in such analyses. How are judicial interpretations impacting the effectiveness of Section 512?

Certain judicial interpretations of "red flag" knowledge, and "willful blindness" under the DMCA have significantly undermined the effectiveness of Section 512.¹⁰¹ These decisions have given rise to a perverse universe where services are incentivized to take efforts to blind themselves to what is occurring over their services, and to take no action to prevent it. This is precisely the opposite of Congressional intent to "preserve the strong incentives for service providers and copyright owners to detect and deal with copyright infringements that take place in the digital networked environment."¹⁰²

Congress intended that the safe harbors only be used by passive, neutral actors. The red flag provision was designed to ensure that result. Thus, a "copyright owner could show that the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly, at the time the directory provider viewed it, a 'pirate' site . . . where sound recordings, software, movies or books were available for unauthorized downloading, public performance or public display."¹⁰³ As such, the statute makes clear that the limitation is conditioned upon,

¹⁰⁰ See, e.g., *Henley v. Devore*, 733 F. Supp. 2d 114 (C.D. Cal. 2010); see also Daniel Kreps, *Don Henley Settles Suit Against California Rep. Chuck DeVore*, ROLLING STONE (Aug. 5, 2010), <http://www.rollingstone.com/music/news/don-henley-settles-suit-against-california-rep-chuck-devore-20100805#ixzz44Jn8C0EB>.

¹⁰¹ See, e.g., *UMG II*, 665 F. Supp. 2d 1099, *aff'd*, *UMG IV*, 667 F.3d 1022; *Viacom III*, 940 F. Supp. 2d at 115; *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500 (S.D.N.Y. 2013), *reconsideration granted in part, reconsideration denied in part*, 972 F. Supp. 2d 537 (S.D.N.Y. 2013).

¹⁰² Report of House Commerce Committee on H.R. 2281, the Digital Millennium Copyright Act, H.R. Rep. No. 105-551, pt. 2, 49 (1998).

¹⁰³ Staff of House Committee on the Judiciary, 105th Cong., Section-By-Section Analysis of H.R. 2281 as Passed by the United States House of Representatives on August 4, 1998, at 33 (Comm. Print 1998), *reprinted in* 46 J. Copyright Soc'y U.S.A. 635 (1999) ("Manager's Rep.").

among other things, taking certain action expeditiously upon “becoming aware of facts or circumstances from which infringing activity is apparent.”¹⁰⁴

Red Flag Knowledge. Commentators have stated that it is reasonable to construe the red flag prong as referring to general infringing activity.¹⁰⁵ Further legislative history clarifies awareness of the facts or circumstances in question should be determined on a subjective standard, but that an objective standard should be used to determine whether “infringing activity is apparent” based on those facts or circumstances.¹⁰⁶ Moreover, “apparent” under Section 512(c)(1)(A)(ii) “does not mean ‘in fact illegal,’ nor does it mean ‘conclusively exists.’”¹⁰⁷

Despite this, the courts in *Veoh* and *Viacom* misapplied the statute to virtually read the red flag prong out of the law. As noted in response to Question 14 above, in *Veoh*, the plaintiff cited several aspects from which a jury could reasonably find that infringing activity was apparent, including various articles that noted Veoh was a haven for pirated content and that the CEO of Veoh was aware that Veoh hosted unauthorized content.¹⁰⁸ Nonetheless, the court granted summary judgment to the defendant by misconstruing the plain meaning of the statute and the relevant legislative history.¹⁰⁹

While the *Viacom* court acknowledged that the jury “could find that the defendants . . . welcomed copyright-infringing material being placed on their website,” it nonetheless decided that the red flag provision requires “knowledge of specific and identifiable infringements of particular items”.¹¹⁰ This result simply does not square with legislative intent nor a proper construction of the difference between actual, specific knowledge of “the infringing activity” versus awareness that general “infringing activity” is present.¹¹¹ Furthermore, as discussed above, it reads out of the statute any meaningful way to provide knowledge of infringement through a “representative list”.

Critics argue that any requirement under the red flag prong to require action absent express URL-by-URL identification of the infringement is inconsistent with Section 512(m)(i). This is incorrect, and ignores the other provisions of the statute. While Section 512(m)(i) does not obligate a service provider to generally monitor its service or affirmatively seek facts indicating infringing activity, this does not mean that providers can avoid taking expeditious action once they have awareness of infringing activity or have received a representative list of infringement. As noted in legislative history, the “no monitoring” provision was “designed to protect the privacy of Internet

¹⁰⁴ *Nimmer*, § 12:B.04, *supra* n. 86 (“In short, the ‘actual knowledge’ prong is reasonably construed to refer to specifics, whereas the ‘red flag’ prong deals with generalities.”).

¹⁰⁵ *Id.*

¹⁰⁶ House Judiciary Committee Report, H.R. Rep. No. 105-551, at 53; Senate Judiciary Committee Report, S. Rep. No. 105-190, at 44.

¹⁰⁷ Jane C. Ginsburg, *Separating the Sony Sheep from the Grokster Goats*, 50 ARIZ. L. REV. 577, 598 (2008).

¹⁰⁸ *UMG II*, 665 F. Supp. 2d 1099; *aff’d UMG III*, 667 F.3d 1022; *UMG IV*, 718 F.3d at 1014.

¹⁰⁹ *UMG II*, 665 F. Supp. 2d 1099.

¹¹⁰ *Viacom*, 718 F. Supp. 2d at 523.

¹¹¹ *See Nimmer*, *supra* n. 86.

users.”¹¹² It was not intended to discourage the service provider from monitoring its service for infringing material, and certainly it was never intended to permit providers to continue to operate with impunity despite knowledge of wide- ranging infringing activity over their services.

These misinterpretations of “red flag” knowledge further widen the schism between what Congress intended – incentives for service providers and content owners to cooperate to detect and deal with infringement – and actual practice in today’s market place.

Willful Blindness. With respect to “willful blindness”, even the *Viacom* court recognized that, if a service provider is aware of a high probability of infringement on its system but then successfully turns a blind eye to avoid confirming that fact, there will rarely, if ever, be evidence of the provider’s awareness of “particular infringing transactions.”¹¹³ That is why the willful blindness doctrine, to prevent an actor from benefiting from its misconduct, serves as a substitute “to demonstrate” the required knowledge or awareness.¹¹⁴ To rule otherwise, as the *Vimeo* district court erroneously did,¹¹⁵ rewards willful blindness and “essentially empties any significance from the willful blindness inquiry.”¹¹⁶

As a consequence of these judicial decisions, rather than providing incentives for cooperation, the DMCA has provided incentives for service providers to turn a blind eye to infringement, or even to build willful blindness into their business models, contrary to the diligence expected in nearly any other business environment.¹¹⁷ This has resulted not only in increased inefficiencies in the DMCA regime,¹¹⁸ and market distortions in the value of music,¹¹⁹ but also in various rogue sites claiming DMCA protection when in fact, they are intentionally gaming the system. This is the exact opposite of Congressional intent.

¹¹² House Judiciary Committee Report, H.R. Rep. No. 105-551, at 64-65; Senate Judiciary Committee Report, S. Rep. No. 105-190, at 55.

¹¹³ *Viacom II*, 676 F. 3d at 35.

¹¹⁴ *Id.*

¹¹⁵ *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500 (S.D.N.Y. 2013).

¹¹⁶ *Nimmer* § 12B.04[A][1][b][iii], *supra* n. 86.

¹¹⁷ See Terry Hart, *Grooveshark is Done*, COPYHYPE (Oct. 1, 2014),

<http://www.copyhype.com/2014/10/grooveshark-is-done/> (Grooveshark instructed its employees to create user accounts and to upload infringing files to the site, knowing that the business “depended on the use of infringing content”); see also William Hensley, *Copyright Infringement Pushin’: Google, YouTube, and Viacom Fight for Supremacy in the Neighborhood that may be Controlled by the DMCA’s Safe Harbor Provision*, 51 IDEA 607, 626 (2011) (“YouTube’s business model was designed to maximize the number of site viewers in order to increase advertising revenue to attract a buyer. To increase the number of viewers, they needed infringing material.”). The DMCA’s current provision providing that monitoring is not required was intended to apply to passive ISPs who otherwise meet the statutory eligibility tests for the safe harbors – not to shield ISPs operating with full awareness of the widespread presence of infringing content and indeed active inducement of posting of such content.

¹¹⁸ Please see responses to Questions 6, 16 and 26.

¹¹⁹ Please see response to Question 4.

20. Assess courts’ interpretations of the “financial benefit” and “right and ability to control” standards under the Section 512 safe harbors. How are judicial interpretations impacting the effectiveness of Section 512?

Certain judicial interpretations of the “financial benefit” and “right and ability to control” standards under the Section 512 safe harbors have similarly upset the balance Section 512 was intended to strike.

In discussing this condition, Congress recommended that “courts should take a common-sense, fact-based approach, not a formalistic one” to determining if there is a financial benefit.¹²⁰ For example, Congress stated that a service provider would be ineligible for the safe harbor under this prong where “the value of the service lies in providing access to infringing material.”¹²¹ Congress further noted that the “right and ability to control” provision was intended to preserve existing case law that examines all relevant aspects of the relationship between the primary and secondary infringer.¹²²

In considering the “financial benefit” prong, courts previously stated they should apply the same standard used for vicarious copyright infringement.¹²³ Taking that to heart, courts should look to the Ninth Circuit’s decision in *Fonovisa*¹²⁴ for a practical model.¹²⁵ In *Fonovisa*, vicarious liability was imposed because the availability and sale of infringing goods enhanced the attractiveness of the venue to potential customers and the provider, Cherry Auction, had the right and ability to terminate the vendors for any reason and/or control their activities. Cherry Auction’s provision of the site and facilities for known infringing activity was sufficient to establish contributory liability as well.

Yet under existing DMCA case law, very few defendants have been found ineligible for the safe harbor due to the financial benefit prong.¹²⁶ For example, defendants more closely resembling digital versions of Cherry Auction were able to claim the safe harbor, with courts deciding that “something more” is now required to show ineligibility under the financial benefit prong.¹²⁷ Because of this, at least one court suggested that only a very high standard of actual control would satisfy the “right and ability to control prong”.¹²⁸

¹²⁰ House Commerce Committee Report, H.R. Rep. No. 105-551, at 54 (1998).

¹²¹ House Judiciary Committee Report, H.R. Rep. No. 105-551, at 54; Senate Judiciary Committee Report, S. Rep. No. 105-190, at 44-45.

¹²² House Commerce Committee Report, H.R. Rep. No. 105-551, at 25 (1998).

¹²³ *CCBill*, 488 F.2d at 1117.

¹²⁴ 76 F.3d 259 (9th Cir. 1996).

¹²⁵ *Id.*

¹²⁶ To be sure, in a few egregious cases, such as *Columbia Pictures Indus. v. Gary Fung*, defendants have been found to have such financial benefit and right and ability to control. 710 F.3d 1020 (9th Cir. 2013).

¹²⁷ *Hendrickson v. eBay, Inc.*, *supra* n. 23; *see also*, *Viacom*, 718 F. Supp. 2d 514.

¹²⁸ The court implied that only the following type of evidence would be sufficient to show the right and ability to control prong: “evidence that YouTube induced its users to submit infringing videos, provided users with detailed instructions about what content to upload or edited their content, prescreened submissions for quality, steered users to infringing videos, or otherwise interacted with infringing users to a point where it might be said to have participated in their infringing activity.” *Viacom III*, 940 F. Supp. 2d at 121. The *Veoh* case went further, suggesting erroneously that in order to meet a standard intended to

Additionally, in another troubling decision (now on appeal), a federal court in California rewrote from whole cloth a well-established aspect of the financial benefit prong of vicarious infringement. It is black letter law that the financial benefit requirement can be met by, among other things, showing that “the availability of infringing material ‘acts as a ‘draw’ for customers.’”¹²⁹ However, in *Perfect 10, Inc. v. Giganews, Inc.*,¹³⁰ the district court, citing no authority, held that a plaintiff must also demonstrate that its own works, or its category of works, acted as a specific draw to an infringing service.¹³¹ The court so held notwithstanding its recognition that the defendant service in that case was “awash in copyrighted material,” including, “staggering amounts of copyrighted works owned by movie producers and television networks.”¹³²

These judicial interpretations further weaken the statutory conditions that were intended to ensure the safe harbor was only available for passive actors. Instead, the bar has been set so high, services feel they can profit from infringing content with near impunity. This is not what Congress intended, and the law must be rebalanced.

21. Describe any other judicial interpretations of Section 512 that impact its effectiveness, and why.

We take this opportunity to highlight one case in particular, *Lenz v. Universal Music Corp.*¹³³ In that case, contrary to Congressional intent and the weight of authority concerning who has the burden of claiming and proving fair use, the court held that a copyright holder must subjectively consider fair use before submitting a DMCA notice. This unique decision, and the fanfare that has followed it, is quite remarkable considering that other courts have expressly rejected that view,¹³⁴ and that the Supreme Court has

comport with general vicarious liability standards, the defendant’s conduct would need to rise to the level of inducement. *Veoh Networks*, 586 F. Supp. 2d at 1150.

¹²⁹ *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d at 1023 (quoting *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 263- 64 (9th Cir. 1996)); *see also Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004) (“regardless of how substantial the benefit is in proportion to a defendant’s overall profits”) (emphasis omitted).

¹³⁰ 2014 WL 8628034 (C.D. Cal. Nov. 14, 2014) (“*Giganews*”).

¹³¹ *Id.* at *3-4.

¹³² *Id.* at *4.

¹³³ 572 F. Supp. 2d 1150, 1154-55 (N.D. Cal. 2008) (“*Lenz I*”) (denying motion to dismiss); 2008 U.S. Dist. LEXIS 91890 (N.D. Cal. Oct. 28, 2008) (“*Lenz II*”) (denying motion for interlocutory appeal); 2010 U.S. Dist. LEXIS 16899 (N.D. Cal. Feb. 25, 2010) (“*Lenz III*”) (granting plaintiff’s motion for partial summary judgment on affirmative defenses); 2013 U.S. Dist. LEXIS 9799 (N.D. Cal. Jan. 24, 2013) (“*Lenz IV*”) (denying motions for summary judgment).

¹³⁴ *See Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333, 344 (D. Mass. 2013) (rejected view that fair use had to be considered prior to sending a DMCA notice, noting that “To have required [that] would have put the takedown procedure at odds with Congress’s express intent of creating an ‘expeditious[,]’ ‘rapid response’ to ‘potential infringement’ on the Internet” and that “It is also reasonable to assume that Congress was aware well prior to the passage of the DMCA that the Supreme Court had made clear that the burden of proof for a fair use defense rests on the accused infringer.”); *see also Ouellette v. Viacom*, 2011 U.S. Dist. Lexis 52570, at *15 (D. Mont. 2011) (noting that in establishing the DMCA, “Congress chose not to rewrite or modify the existing doctrines that impose liability for copyright infringement as those doctrines apply to the online world.”).

routinely held that the burden of proof for a fair use defense rests on the accused infringer.¹³⁵

The same court recently amended its ruling by omitting certain provisions that helped content owners satisfy the new and unprecedented requirement placed on the content owners by the court to consider fair use before sending the DMCA notice.¹³⁶

It remains to be seen what impact, if any, this decision, and its recent revision, has on the effectiveness of the DMCA. But at a minimum, it is a clear example of why congressional reform of the DMCA is necessary.

22. Describe and address the effectiveness of repeat infringer policies as referenced in Section 512(i)(A).

Too often, it appears that repeat infringer policies are only paid lip service, or not implemented with any rigor, effectively reducing, if not eliminating, their utility to deter infringement.¹³⁷ Overall, repeat infringer policies are meaningless in a world of anonymous uploading. Some services allow uploads without any registration, and some that require registration ask for nothing more than an email account. RIAA Executive Vice President Brad Buckles observes, “In a world of free anonymous uploading... [to platforms such as] lockers, repeat infringer policies are completely meaningless. The DMCA assumed the service provider was providing a service to the user, but in today’s world the user by uploading content is providing a service/value to the service provider.”

Congress included the repeat infringer condition to ensure that “those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access.”¹³⁸ Significantly, it made this condition a prerequisite to any claim of entitlement to safe harbor protection.¹³⁹ Thus, it should be a linchpin to ensure that infringement on any particular service does not get out of control.

In practice, however, there is little to no transparency into the repeat infringer policies of particular companies or organizations. In today’s environment, it appears that one achieves such transparency only through burdensome litigation. Even once suit is brought, establishing whether or not a service’s repeat infringer policy is compliant usually requires sifting through massive volumes of discovery, building expert reports and soliciting testimony to deconstruct just that one service’s repeat infringer policy. The entire cost and risk of such an endeavor falls on copyright owners even though the result may be obvious (*i.e.*, whatever the service’s repeat infringer policy may be, it is not being “reasonably implemented” when the content owner’s works reappear incessantly from the

¹³⁵ *Harper & Row, Publishers, Inc. v. National Enters.*, 471 U.S. 539, 561 (1985) (“The drafters [of sec. 107] resisted pressures from special interest groups to create presumptive categories of fair use, but structured the provision as an affirmative defense.”).

¹³⁶ *Lenz v. Universal Music Corp.*, 2016 U.S. App. LEXIS 5026 (9th Cir. Mar. 17, 2016).

¹³⁷ Please see responses to Questions 6 and 7 for a discussion of problems with repeat infringement.

¹³⁸ Senate Judiciary Committee Report, S. Rep. No. 105-190, at 52 (1998).

¹³⁹ 17 USC 512 (i)(1)(A).

same source). And because of the complex and lengthy litigation process, companies that want to take advantage of this lack of transparency can continue to profit from infringement of the Music Community's protected content for years.¹⁴⁰

Additionally, some providers encourage their users to seek "retractions" or make up excuses to avoid consistently implementing their repeat infringer policies,¹⁴¹ or appear to have weak or ineffective methods of tracking infringement attributable to one of their customer's accounts.¹⁴² This further dilutes the intended impact of the repeat infringer condition.

In any event, there are high percentages of repeat notices sent to the same services, and their underlying providers.¹⁴³ Change is needed to correct this inequity.

23. Is there sufficient clarity in the law as to what constitutes a repeat infringer policy for purposes of Section 512's safe harbors? If not, what should be done to address this concern?

Though Congress's intent was clear, inconsistency among judicial interpretations of the law have led to confusion and uncertainty regarding the repeat infringer standard.

Where the actions of the defendant are clearly egregious or intentional, some courts have been inclined to find that the defendant failed to implement a repeat infringer policy:

- In *Grooveshark*, the court found that the service failed to meet the requirement of reasonably implementing a repeat infringer policy, because it purposely made it nearly impossible for copyright owners to issue meaningful takedown notices, and purposely failed to keep adequate records of repeat infringement or to strip users of uploading privileges.¹⁴⁴
- In *Disney v. Hotfile*, the court ruled that the defendant was ineligible for the Section 512 safe harbors, noting that the defendant not only failed to comply with its policy of terminating users after two strikes, but also failed to tie infringement notices to user's accounts, "despite receiving

¹⁴⁰ Please see responses to Questions 3 and 4 for a discussion of how Grooveshark continued to profit from its unauthorized exploitation of infringing material while in litigation.

¹⁴¹ See *BMG Rights Mgmt. (US) LLC v. Cox Communs., Inc.*, 2015 U.S. Dist. LEXIS 161091, *56 (E.D. Va. Dec. 1, 2015).

¹⁴² As discussed in response to Question 6 above, RIAA has sent CloudFlare notices of nearly 300,000 infringements in connection with Mp3Skull entities on various Mp3Skull domains following the move from Mp3skull.com. CloudFlare has told us that each of those domains points to the same IP address, yet CloudFlare continues to provide service to Mp3Skull.

¹⁴³ Please see responses to Questions 6 and 13 for a discussion of the number of times infringements were noticed to the same site, service or family of sites, particularly in the case of Mp3Skull, as well as the disturbing lack of change in traffic to rogue site, Mp3Skull, as even after the hosting provider for Mp3Skull was noticed, Mp3Skull simply moved its operations to another hosting provider.

¹⁴⁴ *Grooveshark*, at *102-103 (S.D.N.Y. May 28, 2014), *adopted* 2015 U.S. Dist. LEXIS 38007, *18-19, 30-32 (S.D.N.Y. Mar. 25, 2015).

over eight million notices for five million users,” including “more than 300 notices each” for dozens of users who were not terminated.¹⁴⁵

- In *BMG v. Cox*, the court found the defendant failed to implement a repeat infringer policy where internal documents revealed that the defendant had a clear policy to intentionally circumvent the DMCA.¹⁴⁶

In other cases, however, it appears that the courts have strained to find the defendant had a compliant repeat infringer policy, even though the facts made the determination suspect.

- In *Perfect 10 v. Giganews*,¹⁴⁷ the court found that the defendant had reasonably implemented a repeat infringer policy, despite evidence that only 46 accounts had been deleted in a year with over 531 million infringing messages.

In some cases, courts have in effect read the repeat infringer policy condition out of the statute altogether.

- In *CCBill*, the court held that a service provider implements a repeat infringer policy if it has a working notification system, a procedure for dealing with DMCA notifications, and it does not actively prevent copyright owners from collecting information needed to issue such notifications.¹⁴⁸ This approach conflates the repeat infringer requirement with the notice-and-takedown process itself, while Congress clearly intended the former as a condition for reliance on the latter to qualify for safe harbor protection.

The DMCA safe harbors were intended to apply only to passive, innocent actors. Too often, courts have instead ruled that unless evidence of deliberate intent to circumvent the DMCA can be established, a clearly ineffective repeat infringer policy will nonetheless be found to be compliant. In order to correct this, Congress must reform the DMCA to provide greater clarity regarding what qualifies as an acceptable repeat infringer policy and what constitutes reasonable implementation of such a policy.

¹⁴⁵ *Disney Enters. v. Hotfile Corp.*, 2013 U.S. Dist. LEXIS 172339, *68-70 (S.D. Fla. Aug. 28, 2013).

¹⁴⁶ *Cox*, *supra* n. 141 (Defendant purported to have a repeat infringer policy, but internal documents revealed that the provider’s true intention was to “hold onto every subscriber we can.” Thus it told its employees to reactivate the accounts of users who had been terminated due to DMCA notices, and to then treat complaints against them as new complaints. Internally, Cox took the position that they would be in compliance with the DMCA provided they “terminate” the user, even if they quickly reactivated the account and restarted the “DMCA ‘counter.’”).

¹⁴⁷ *See, e.g., Giganews*, at 1196 (C.D. Cal. 2014).

¹⁴⁸ *CCBill*, 488 F.3d at 1109-10.

VII. STANDARD TECHNICAL MEASURES

24. Does Section 512(i) concerning service providers' accommodation of "standard technical measures" (including the definition of such measures set forth in Section 512(i)(2)) encourage or discourage the use of technologies to address online infringement?

Section 512(i) concerning service providers' accommodation of STMs has ironically had the negative impact of discouraging the use of technologies to address digital infringement. Because Section 512(i) acts to limit safe harbor protection, service providers have a perverse disincentive to participate in the development of any STMs, even though Congress expressly encouraged the use of STMs.¹⁴⁹

Consider, for example, the USPTO DMCA Best Practices multi-stakeholder forum discussed above in response to Question 15. Despite calls in that forum to discuss improvements to the effectiveness of the DMCA, including through the use of STMs, the misalignment of interests at the forum prevented those discussions from taking place in a meaningful way. This underscores the need for legislative reform to promote the use of STMs.

Currently, a number of reasonably priced, commercially available technical measures exist to identify and protect copyrighted works.¹⁵⁰ As noted in response to Question 15, some of these measures have shown a significant impact in reducing the number of infringements noticed on certain services, and several services have adopted them.

However, while some service providers have implemented such measures, many others feel no obligation to do so because they were developed organically in the market, and not, they argue, through the consensus process set forth in the DMCA for an STM. And, as noted above, service providers currently have no incentive to participate in such a process.

In addition, some have raised concerns that Section 512(i) creates a one size fits all approach to adopting an STM. In today's environment, this may not make sense, as different tools are available to identify and protect different types of copyrighted works, offered at different price points, and that work in different service provider environments. Allowing more flexibility in how those technical measures can be adopted and when they need to be implemented may help create an environment where appropriate STMs can be adopted by particular kinds of service providers to which they best apply.

25. Are there any existing or emerging "standard technical measures" that could or should apply to obtain the benefits of Section 512's safe harbors?

There are practices that are used by several in the industry that should be considered, or used as a model for, STMs. For example, see the response to Question 15

¹⁴⁹ House Judiciary Committee Report, H.R. Rep. No. 105-551.

¹⁵⁰ See, e.g., audiblemagic.com.

for a description of fingerprinting technologies to identify sound recordings and musical works. If other services that allow user-uploaded content involving music adopted robust implementations of these tools, it would help reduce the legal inefficiencies that currently characterize the DMCA notice-and-takedown regime.

Other options that should be explored include efforts to identify and deter dissemination of unauthorized sound recordings through the use of metadata¹⁵¹ as well as implementation of systems that allow rights holders to more easily send takedown notices with bulk URLs.

VIII. REMEDIES

26. Is Section 512(g)(2)(C), which requires a copyright owner to bring a federal lawsuit within ten business days to keep allegedly infringing content offline – and a counter-notifying party to defend any such lawsuit—a reasonable and effective provision? If not, how might it be improved?

As discussed above, Section 512(g)(2)(C), is not a reasonable provision, and is ineffective for the purposes intended.

Consider the statistics offered in response to Question 12 above. Based on that study on one month of data, even though the number of counter-notices received was tiny compared to the number of notices sent, the percentage of those counter-notices that appeared erroneous was over 80%. In that study, under Section 512(g)(2)(C), the rights holder would be obligated to bring over 500 lawsuits in order to protect its intellectual property. And that is based on observations of only a single service during a single month.

The problem is that any currently available solutions are highly un-scalable in the current environment, where technology and data transfer speeds permit millions of users to upload to countless services on a daily basis, and service providers' pecuniary interests make them inclined to favor their users over rights holders. Most artists simply do not have the resources to engage in such a costly, and time compressed litigation.¹⁵² The environment is ripe for abuse by uploaders, and the 10-day rule, among the other statutory provisions discussed in these comments, makes it virtually impossible for rights holders to obtain recourse.

27. Is the limited injunctive relief available under Section 512(j) a sufficient and effective remedy to address the posting of infringing material?

Section 512(j) has proven to be an illusory remedy that has rarely, if ever, been invoked in any meaningful respect. While reasonable, targeted injunctions applied to

¹⁵¹ *Gardner v. Cafepress Inc.*, No. 3:13-cv-1108-GPC-JMA, 2014 US Dist LEXIS 25405 (S.D. Cal. Feb. 26, 2014).

¹⁵² Please see response to Question 18 for a discussion of the cost of litigation and the dearth of artists who have actually sued under the counter-notification provision; *see also*, *Henley*, 735 F. Supp. 2d 114.

Internet intermediaries should be helpful in deterring infringement, particularly repeat infringement, and developing a balanced and healthy marketplace for music, experience up to this point indicates that such injunctions will practically never be meaningfully issued under the DMCA as currently drafted.

The few cases that have addressed Section 512(j) have found the issue of injunctive relief to be moot because the service provider had already removed the infringing material and/or terminated the accounts of the infringers by the time the case was heard.¹⁵³ Further, even if Section 512(j) were applied more commonly, it would not offer much more relief from the whack-a-mole problem than notice-and-takedown measures do. This is particularly true under Section 512(j)(B)(ii), which provides that a court may issue an injunction preventing a Section 512(a) service from providing access to a “specific, identified, online location outside the United States”. While this provision should be read to mean an injunction can be applied to deter infringement from rogue sites, recent court decisions suggest that any proposed injunction broader than a specific URL by URL injunction, even if it included a representative list of the copyrighted works at issue, would be difficult to obtain.

The presence of offshore digital services that make infringing material available to the U.S. market was mainly a theoretical concern in 1998. In 2016, it is a pervasive and intractable reality.¹⁵⁴ Where such sites are hosted or based in one country but target consumers in another — or worldwide — the failure of the host country to take effective action against them imposes costs on and pollutes the markets of its neighbors and trading partners. Increasingly, responsible governments are pushing back against this “offshoring” of enforcement responsibility, by developing means and processes for restricting or blocking access from within their borders to these overseas pirate sites. In due course, the U.S. must join the growing number of its trading partners by stepping up to this problem and providing an effective and reasonable solution, whether or not within the DMCA context. The current provision in Section 512(j) is clearly insufficient.

28. Are the remedies for misrepresentation set forth in Section 512(f) sufficient to deter and address fraudulent or abusive notices and counter notifications?

As discussed in responses to Questions 12 and 26, one study found that only 0.7% of notices were counter-noticed, which suggests that Section 512(f) does deter fraudulent notices by at least some rights-holders. However, the same study found that over 80% of the counter-notices were erroneous, which suggests that Section 512(f) has a much lesser impact on abusive counter-notices.

¹⁵³ See, e.g., *Veoh Networks*, 586 F. Supp. 2d at 1154-1155 (injunction moot because infringing content already removed); *Wolk v. Kodak Imaging Network, Inc.*, 2011 U.S. Dist. LEXIS 27541, *19-21 (S.D.N.Y. Mar. 17, 2011) (defendant already removing material in response to compliant notice, which is essentially what injunction sought).

¹⁵⁴ For a description of dozens of such sites, hosted in numerous foreign jurisdictions, see USTR, *2015 Out-of-Cycle Review of Notorious Markets* (Dec. 2015), available at <https://ustr.gov/sites/default/files/USTR-2015-Out-of-Cycle-Review-Notorious-Markets-Final.pdf>. The sites listed are only a fraction of those nominated by RIAA and other copyright industry organizations as “notorious online marketplaces” engaged in or dedicated to facilitating copyright infringement.

IX. OTHER ISSUES

29. Please provide any statistical or economic reports or studies that demonstrate the effectiveness, ineffectiveness, and/or impact of Section 512's safe harbors.

In addition to the studies and reports cited throughout this submission, please see Appendix D for a list of reports and studies that help address these issues.

30. Please identify and describe any pertinent issues not referenced above that the Copyright Office should consider in conducting its study.

For now, the Music Community omits any response to this question.

X. CONCLUSION

In 1998, the Music Community worked with service providers and Congress to draft and pass the DMCA – a balanced compromise that most believed would address the legitimate concerns of both constituencies. The Music Community believed the DMCA provided their community with reasonable, yet effective means to protect their works against infringing activity on the Internet. The passive intermediaries believed they would be protected from liability that was not facilitated by their services, and the law would provide them with a road to expand their business and the overall vitality of the digital marketplace.

Almost 20 years later, the reality on the ground bears little resemblance to the expectations of the Music Community when the DMCA was passed. The DMCA is arguably the first comprehensive law designed to regulate activity of content owners, passive intermediaries, and users of digital services. However, instead of the carefully balanced law passed by Congress, the DMCA has now become a dysfunctional relic, not suited to the realities of the 21st Century. This is not what Congress or those stakeholders involved in passing the DMCA intended.

Relying on the courts to resolve the problems of the DMCA at this point is unrealistic. Congress must get involved. The Music Community calls on Congress to re-examine the DMCA and to promote reasonable, sensible DMCA reform. The Copyright Office should assist Congress in this process by studying the problematic sections of the law, determining how these provisions have negatively impacted the Music Community, and ultimately advise Congress on how to reform the law in ways that restore the balance between the creative and technology communities that Congress intended to underlie the law from its inception.

The Music Community commits to working with the Copyright Office, Congress and other stakeholders in this legislative process.

Respectfully submitted on behalf of the
Music Community

A handwritten signature in black ink that reads "Jay Rosenthal" followed by a stylized flourish.

Jay Rosenthal, Esq.
Steven Metalitz, Esq.
Mitchell Silberberg & Knupp LLP
1818 N Street, NW
8th Floor
Washington, DC 20036
jar@msk.com
met@msk.com
March 31, 2016

Appendix A

Music Community Members

A2IM

A2IM is a 501(c)(6) not-for-profit trade organization headquartered in New York City representing a broad coalition of 391 Independently-owned American music labels. The organization represents these independently owned small and medium-sized enterprises' (SMEs) interests in the marketplace, in the media, on Capitol Hill, and as part of the global music community. In doing so it supports a key segment of America's creative class that represents America's diverse musical cultural heritage. Billboard Magazine, using Nielsen SoundScan data, identified the Independent music label sector as 34.4 percent of the music industry's U.S. recorded music sales market in 2015 based on copyright ownership, making Independent labels collectively the largest music industry segment.

American Society of Composers, Authors and Publishers

The American Society of Composers, Authors and Publishers (ASCAP) is a membership association of more than 565,000 US composers, songwriters, lyricists and music publishers of every kind of music. Through agreements with affiliated international societies, ASCAP also represent hundreds of thousands of music creators worldwide. ASCAP is the only US performing rights organization created and controlled by composers, songwriters and music publishers, with a Board of Directors elected by and from its membership.

ASCAP protects the rights of ASCAP members by licensing and distributing royalties for the non-dramatic public performances of their copyrighted works. ASCAP's licensees encompass all who want to perform copyrighted music publicly.

Americana Music Association

The Americana Music Association is a professional non-profit trade organization whose mission is to advocate for the authentic voice of American Roots Music around the world. The Association curates events throughout the year including the annual Americana Music Festival and Conference in Nashville, the acclaimed Americana Honors & Awards program (and PBS special) and "Americana NYC" in partnership with Lincoln Center, New York City.

Broadcast Music, Inc.

BMI was founded in 1939 by forward-thinkers who wanted to represent songwriters in emerging genres, like jazz, blues and country, and protect the public performances of their music. Operating on a non-profit-making basis, BMI is now the largest music rights organization in the U.S. and is still nurturing new talent and new music.

BMI is the bridge between songwriters and the businesses and organizations that want to play their music publicly. As a global leader in music rights management, BMI serves as an advocate for the value of music, representing more than 10.5 million musical works created and owned by more than 700,000 songwriters, composers and music publishers.

Christian Music Trade Association

Established in 1993, the Christian Music Trade Association is a non-profit organization that exists to build community and cooperation among Christian & Gospel music industry leadership in order to address mutual issues and to maximize Christian/Gospel music's impact on culture. The CMTA supports and promotes all styles of gospel music including pop, black gospel, hip hop, rock, country, southern gospel and more.

Church Music Publishers Association

The Church Music Publishers Association (CMPA), Nashville, TN, is an organization of North American and international publishers of Christian and other religious music that promotes worldwide copyright information, education, and protection. Founded in 1926, CMPA represents 56 member publishers.

Global Music Rights

Global Music Rights was founded in 2013 by Irving Azoff and represents music rights holders for the licensing of their public performances. Former Performing Rights Organization (PRO) executives Randy Grimmatt and Sean O'Malley run operations and bring with them more than 30 years of collective experience in music publishing. Global Music Rights offers licensing, distribution and collection services for the exclusive rights granted to music creators and owners by copyright law.

The Latin Academy of Recording Arts & Sciences, Inc.

The Latin Recording Academy is a non-profit international membership based U.S. organization comprised of thousands of recording artists, musicians, songwriters, producers and other creative and technical professionals. The organization is dedicated to improving the quality of life and cultural condition for Latin music and its makers. In addition to producing the Latin GRAMMY Awards honoring excellence in the recorded arts and sciences, The Latin Recording Academy provides educational and outreach programs for the Latin music community.

Music Managers Forum – United States

The Music Managers Forum (MMF-US) provides a platform to connect, enhance, and reinforce the expertise and professionalism of music managers. Our goal is to further the interests of managers and their artists in all fields of the music industry, including live performance, recording and music publishing matters.

While many up and coming managers cannot easily have their voices heard or their views recognized, the MMF-US has a vital role to play in ensuring that the industry evolves fairly and profitably for all who work in the management industry and their clients. It is the goal of the MMF-US to make sure managers voices are heard. As the industry continues to evolve, the MMF-US endeavors to help its members to stay ahead of the curve.

Music Publishers Association

Founded in 1895, the Music Publishers Association is the oldest music trade organization in the United States, fostering communication among publishers, dealers, music educators, and all ultimate users of music. This non-profit association addresses itself to issues pertaining to every area of music publishing with an emphasis on the issues relevant to the publishers of print music for concert and educational purposes.

Nashville Songwriters Association International

The Nashville Songwriters Association International (NSAI) is the world's largest not-for-profit songwriters trade association. Established in 1967, the membership of more than 5,000 active and professional members spans the United States and seven other countries. NSAI is dedicated to protecting the rights of and serving aspiring and professional songwriters in all genres of music.

National Academy of Recording Arts and Sciences

Established in 1957, The Recording Academy is an organization of musicians, songwriters, producers, engineers and recording professionals that is dedicated to improving the cultural condition and quality of life for music and its makers. Internationally known for the GRAMMY Awards® — the preeminent peer-recognized award for musical excellence and the most credible brand in music — The Recording Academy is responsible for groundbreaking professional development, cultural enrichment, advocacy, education and human services programs. The Academy continues to focus on its mission of recognizing musical excellence, advocating for the well-being of music makers and ensuring music remains an indelible part of our culture.

National Music Publishers' Association

Founded in 1917, the National Music Publishers' Association (NMPA) is the largest music publishing trade association in the United States and the voice of music publishers and their songwriter partners. Its mission is to protect, promote, and advance the interests of music's creators on the legislative, judicial, and regulatory fronts.

Recording Industry Association of America

The Recording Industry Association of America (RIAA) is the trade organization that supports and promotes the creative and financial vitality of the major music companies. Its members are the music labels that comprise the most vibrant record industry in the world. RIAA members create, manufacture and/or distribute

approximately 85% of all legitimate recorded music produced and sold in the United States.

Rhythm and Blues Foundation

The Rhythm & Blues Foundation is the pre-eminent non-profit organization dedicated to the historical and cultural preservation of Rhythm & Blues music. It provides financial and medical assistance, educational outreach, performance opportunities and archival activities to Rhythm & Blues artists and their fans.

Screen Actors Guild – American Federation of Television and Radio Artists

Screen Actors Guild – American Federation of Television and Radio Artists (SAG-AFTRA) represents more than 160,000 actors, announcers, broadcast journalists, dancers, DJs, news writers, news editors, program hosts, puppeteers, recording artists, singers, stunt performers, voiceover artists and other media professionals. SAG-AFTRA members are the faces and voices that entertain and inform America and the world. With national offices in Los Angeles and New York, and local offices nationwide, SAG-AFTRA members work together to secure the strongest protections for media artists into the 21st century and beyond.

SESAC Holdings, Inc.

SESAC is a music rights organization that administers public performance, mechanical, synchronization and other rights. The combination of SESAC's performing rights business with The Harry Fox Agency's recently acquired mechanical rights business and SESAC's micro-licensing and network monetization affiliate, Rumblefish, allows SESAC to make licensing simpler, more efficient and more transparent. As SESAC undertakes this transformation, SESAC's performing rights business will continue to represent a renowned roster of affiliates including Bob Dylan, Mumford & Sons, Neil Diamond, Green Day, Mariah Carey, Lady Antebellum, Alt-J among many others.

SoundExchange

SoundExchange is the independent non-profit collective management organization representing the entire recorded music industry. The organization collects statutory royalties on behalf of over 110,000 recording artists and master rights owners accounts for the use of their content on satellite radio, Internet radio, cable TV music channels and other services that perform sound recordings over noninteractive digital music services. The Copyright Royalty Board, created by Congress, has entrusted SoundExchange as the sole entity in the United States to collect and distribute statutory digital performance royalties from more than 2,500 services. Since 2003, SoundExchange has paid out over \$3 billion in royalties.

Appendix B

The Law and Policy Landscape Pre-DMCA

A. The White Paper

In February 1993, President Clinton formed the Information Infrastructure Task Force (“IITF”), chaired by Commerce Secretary Ron Brown, and assigned it the task of articulating Administration policy related to the emergence of the Internet as a commercial and cultural force. A National Advisory Council was established within the Commerce Department to advise the Secretary on relevant issues, including intellectual property rights. Bruce Lehman, Assistant Secretary of Commerce, chaired the Working Group on Intellectual Property Rights (the “Working Group”).

The Working Group issued a Federal Register Notice requesting comments in October 1993 and held hearings in November 1993. Following the hearings, the Working Group published in July 1994 a draft report on policy proposals, commonly referred to as “the Green Paper.” More public comments were received and then more hearings took place in September 1994. One year later, in September 1995, the Working Group published “Intellectual Property and the National Information Infrastructure,” which is commonly referred to as “the White Paper.”¹

During this two-and-one-half-year period, lawsuits involving placement of infringing copies of works on publicly accessible electronic bulletin-board systems (“BBS”) began to move through the courts.² The first two cases to result in published opinions alarmed technology companies who provided access to the Internet and various BBS services. These cases held that an Internet service provider could be strictly liable for direct infringement, even where a provider’s subscriber, rather than the provider itself, uploaded the infringing copies.³

In the White Paper, the Working Group noted these cases, as well as two pending cases,⁴ and considered their implications. The report explained the views expressed by Internet service providers:

¹ “Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights,” Information Infrastructure Task Force (Sept. 1995), <http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf> (“The White Paper”).

² Also during this time, a criminal case involving placement of unauthorized copies of software programs on a BBS resulted in an acquittal based on a judicial interpretation of a statutory requirement that only infringement for commercial advantage or private financial gain attracted criminal liability. *See United States v. LaMachia*, 871 F. Supp. 535 (D. Mass. 1994). Congress reacted by amending the Copyright Act to allow for criminal penalties where Internet dissemination results in significant harm to a copyright owner, even if the infringer did not profit. *See The No Electronic Theft Act*, Pub. L. No. 105–147 (1997).

³ *See Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993); *Sega Enterprises Ltd. v. MAPHIA*, 857 F. Supp. 679, 683 (N.D. Cal. 1994). A third case, which went unmentioned in the White Paper, also held a BBS operator directly liable. *See Central Point Software, Inc. v. Nugent*, 903 F. Supp. 1057 (E.D. Tex. 1995).

⁴ *See Frank Music Corp. v. CompuServe Inc.*, No. 93 Civ. 8153 (S.D.N.Y. filed Nov. 29, 1993) (settled Nov. 8, 1995); *Netcom*, 907 F. Supp. 1361. For an academic discussion of the cases from that time period,

Some have a view that on-line service providers, such as bulletin board operators, should be exempt from liability or given a higher standard for liability, such as imposing liability only in those cases where infringement was willful and repeated or where it was proven that the service provider had both “actual knowledge” of the infringing activity and the “ability and authority” to terminate such activity. The latter proposed standard would combine the contributory infringement standard with the requirements for vicarious liability and apply it to all infringements (including direct infringements) of the service provider.⁵

However, the Working Group declined to recommend the changes to the law proffered by the large Internet service providers:

It would be unfair – and set a dangerous precedent – to allow one class of distributors to self-determine their liability by refusing to take responsibility. This would encourage intentional and willful ignorance. Whether or not they choose to reserve the right to control activities on their systems, they have the right. Service providers expect compensation for the use of their facilities – and the works thereon – and have the ability to disconnect subscribers who take their services without payment. They have the same ability with respect to subscribers who break the law. Exempting or reducing the liability of service providers prematurely would choke development of marketplace tools that could be used to lessen the risk of liability and the risk to copyright owners, including ... educating their subscribers about infringement and using technological protections, such as tracking mechanisms.⁶

In support of its conclusion, the Working Group also offered the following prescient reasoning.

Circumstances also vary greatly among service providers. ... There are those that try to prevent and react when notified and those that encourage infringing activity. Different service providers play different roles – and those are changing and being created virtually every day. At this time in the development and change in the players and roles, it is not feasible to identify *a priori* those circumstances or situations under which service providers should have reduced liability.⁷

The White Paper included proposed, draft legislation, which was introduced almost immediately as the National Information Infrastructure Copyright Protection Act of 1995.⁸ However, the legislation, which lacked any liability limitations for Internet

see I. Trotter Hardy, *The Proper Legal Regime For Cyberspace*, 55 U. PITT. L. REV. 993 (1994); Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Services*, 13 CARDOZO ARTS & ENT. L.J. 345 (1993).

⁵ The White Paper at 114. See also *Public Hearings Explore IP and Fair Use on Information Highway*, 48 PAT. TRADEMARK & COPYRIGHT J. (BNA) 567 (Sept. 29, 1994) (describing testimony of Ellen Kirsh of America Online).

⁶ The White Paper at 123.

⁷ *Id.* at

⁸ See H.R. 2441, and S. 1284.

service providers, failed to become law. This failure was due, in part, to opposition from large Internet service providers, who wanted the immunity that the Working Group viewed as counter-productive.⁹

B. Developing Case Law

Meanwhile, several cases were decided that altered the landscape significantly. The first and the most important was *Religious Tech. Center v. Netcom On-Line Communications*,¹⁰ in the Northern District of California. In this decision, the court concluded that the Copyright Act did not impose direct liability on a person who did not engage in a volitional act that violated one of the exclusive rights provided to copyright owners in 17 U.S.C. § 106.¹¹ In so doing, the court expressly disagreed with *Playboy Enterprises v. Frena*¹² and *Sega v. MAPHIA*¹³ on this point of law. The court stated: “Where the infringing subscriber is clearly directly liable for the same act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet.”¹⁴

However, the *Netcom* court did not absolve Internet service providers of all liability in connection with their subscribers’ conduct. Instead, the court carefully parsed theories of secondary liability. The court concluded that summary judgment could not be granted in favor of Netcom because Netcom continued to provide access to the direct infringer at issue after receiving a complaint letter from the plaintiff.¹⁵ Concluding that “[a]lthough a mere unsupported allegation of infringement by a copyright owner may not automatically put a defendant on notice of infringing activity, Netcom’s position that liability must be unequivocal is unsupportable,” the court also said that the notice provided by the copyright owner should “have triggered an investigation into whether there was infringement.”¹⁶

With respect to vicarious liability, the court concluded an issue of fact existed regarding Netcom’s right and ability to control infringing conduct because the evidence indicated that “with an easy software modification Netcom could identify postings that contain particular words or come from particular individuals” and that Netcom had “acted to suspend subscribers’ accounts on over one thousand occasions ... for commercial advertising, posting obscene materials, and off-topic postings.”¹⁷ However, the court concluded that the plaintiff’s vicarious claim failed because the plaintiff introduced no evidence to show that Netcom profited from the infringement in any manner other than receiving a fixed fee for access provision, which the court compared to a landlord

⁹ See Robert Levine, *FREE RIDE*, 15-31 (Double Day, 1st. ed. 2011) (describing negotiations related to bills).

¹⁰ *Netcom*, 907 F. Supp. 1361.

¹¹ *Id.*

¹² *Frena*, 839 F. Supp. at 1554.

¹³ *MAPHIA*, 857 F. Supp. at 683.

¹⁴ *Netcom*, 907 F. Supp. 1361. at 1372

¹⁵ *Id.* at 1374.

¹⁶ *Id.*

¹⁷ *Id.* at 1376.

receiving rent payments (a circumstance that traditionally did not result in vicarious liability).¹⁸ The court found that the plaintiff failed to show that Netcom attracted subscribers by advertising lax copyright standards because the evidence introduced did not adequately support that such a strategy was implemented.¹⁹

In sum, *Netcom*'s holdings may be stated as follows:

- An Internet service provider does not commit direct infringement by routing transmissions or temporarily storing content at the direction of a user because no volition is involved in such conduct.
- Contributory liability may be imposed where an Internet service provider is provided with notice of infringement on its system but fails to properly investigate and put a stop to infringement of the relevant works or by the user at issue.
- Vicarious liability may be imposed where an Internet service provider is capable of implementing technological methods of identifying infringing conduct and terminating the access and use privileges of specific users but fails to do so while financially benefitting either from payments directly related to accessing or posting specific infringing content or by using infringing content to attract users.

Immediately following *Netcom*, courts considering BBS cases almost unanimously elected to adopt its approach to direct liability, rather than the approach of *Frena* and *MAPHIA*.²⁰ Nevertheless, some cases, distinguished their facts from *Netcom*, found direct infringement occurred due to the extensive involvement of defendants in the conduct at issue.²¹ Where defendants purposefully sought to create Internet destinations where users could access infringing material for a price, and the defendants actively participated in the collection of content for that purpose, they were found directly liable.²²

For example, in *Playboy Enterprises v. Webworld*, the defendants selected specific adult-oriented news groups to copy and then used software to crawl the content, strip out the text, and create thumbnail and full-size copies of images. The defendants then offered users access to these images at subscription prices. Many of the images were infringing copies owned by Playboy. The defendants attempted to compare themselves to *Netcom*, but the court disagreed. "Webworld did not sell access; it sold adult images. ... Webworld did not function as a passive conduit of unaltered

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ See, e.g., *Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distributors and Northwest Nexus, Inc.*, 983 F. Supp. 1167 (D. Ill. 1997); *Sega Enterprises Ltd. v. Sabella*, No. C 93-04260 CW, 1996 U.S. Dist. LEXIS 20470 (N.D. Cal. Dec. 18, 1996); *Playboy Enterprises, Inc. v. Webworld, Inc.*, 991 F. Supp. 543 (N.D. Tex. 1997), *aff'd* 168 F.3d 486 (5th Cir. 1999); *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Oh. 1997). In fact, in an opinion on summary judgment, the *MAPHIA* court itself agreed with *Netcom*, despite its earlier decision on a preliminary injunction motion. *MAPHIA*, 948 F. Supp. 923.

²¹ See, e.g., *Russ Hardenburgh, Inc.*, 982 F. Supp. 503; *Webworld, Inc.*, 991 F. Supp. 54, *aff'd* 168 F.3d 486.

²² *Id.*

information. Instead, Webworld functioned primarily as a store, a commercial destination within the Internet.”²³

The court also rejected the defendants’ attempt to claim ignorance of the copyrighted nature of the content at issue. “Clearly, a newsgroup named, for example, “alt.sex.playboy” or “alt.mag.playboy” might instantly be perceived as problematic from the standpoint of federal copyright law. Alternatively, Webworld might simply have refrained from conducting business until it had developed software or a manual system of oversight to prevent, or at least to minimize the possibility of, copyright infringement.”²⁴

In *Playboy Enterprises v. Russ Hardenburgh*, the defendants were also actively involved in infringement. They actively encouraged users to upload infringing images by offering users free downloads in exchange for uploads. The defendants also screened images prior to electing to post them and charged a subscription price to access certain images that were not otherwise publicly accessible. The court found these factors justified a finding of direct infringement, concluding that “[i]t is inconsistent to argue that one may actively encourage and control the uploading and dissemination of adult files, but cannot be held liable for copyright violations because it is too difficult to determine which files infringe upon someone else’s copyrights.”²⁵

Post-*Netcom* BBS cases also applied approaches to secondary liability in a manner similar to *Netcom*. For example, in *Marobie v. National Association of Fire Equipment Distributors*,²⁶ the court acknowledged that hosting a website could lead to contributory liability. The court declined to grant summary judgment for the defendant because, based on the evidence presented, it was unclear whether Northwest knew that any material on the website was copyrighted and, “if it did know, when it knew.”²⁷

In *Sega v. Sabella*,²⁸ the court held the defendant contributorily liable because the plaintiff proved the defendant had knowledge of the infringement in the following manners:

Here, Sega has established the following: Sabella was the system operator of her BBS; files on Sabella’s BBS were labeled as Sega Genesis games; and Sabella had the ability to track user uploads and downloads of these files. Additionally, postings on her BBS indicated that downloadable files were playable and warned that she and the co-sysop “read the user log several times a day.”²⁹ These facts establish the inference that Sabella had reason to know of her users’ infringing activity.³⁰

In *Playboy Enters. v. Russ Hardenburgh*, the court also found the defendant contributorily liable. The court found knowledge and material contribution to

²³ 991 F. Supp. 543 at 552.

²⁴ *Id.* at 553.

²⁵ 982 F. Supp. 503 at 513.

²⁶ 983 F. Supp. 1167.

²⁷ *Id.* at 1178.

²⁸ 1996 U.S. Dist. LEXIS 20470.

²⁹ *Id.* at *23-24.

³⁰ *Id.* at 24.

infringement based on the following facts (which appear to mix and match things relevant to both contributory and vicarious liability):

Defendants clearly induced, caused, and materially contributed to any infringing activity which took place on their BBS. Defendants admit that they encouraged subscribers to upload information including adult files. Defendants admit that they benefitted from having more files available to their customers. Also, Defendants had at least constructive knowledge that infringing activity was likely to be occurring on their BBS. Defendants were aware that PEI was enforcing its copyrights against BBS owners. Moreover, Playboy Magazine is one of the most famous and widely distributed adult publications in the world. It seems disingenuous for Defendants to assert that they were unaware that copies of photographs from Playboy Magazine were likely to find their way onto the BBS. Defendants are liable for contributory copyright infringement.³¹

i. The Technology Landscape

The DMCA was written to address a technological landscape that differs markedly from what prevails today. This was true both with respect to the scope and volume of infringement, and the strength and robustness of the technical tools available to combat it.

The online environment of 1998 was certainly replete with infringing material, especially for relatively small files of text, small software programs, and audio recordings, which the existing infrastructure for data storage and transmission could readily accommodate. But the volume of infringing materials was, by today's standards, relatively minimal. The BBS systems described in the cases decided prior to 1998 stored and made available dozens or hundreds of works, but not the millions or tens of millions now featured on numerous user-generated content sites. Similarly, this was an environment in which the process for gathering, storing and disseminating infringing copies was more of a craft than an industry, and automation of the process was comparatively limited. A pirate BBS could depend upon the manual, copy-by-copy stripping of copyright notices from individual images.

Although the Internet was beginning to attract millions of users by the late 1990s, it was very different from the omnipresent commercial and cultural powerhouse we know today. Probably the most significant differences relate to speed and storage space. In the late 1990s, dial-up access was the standard. It took multiple seconds just to move from webpage to webpage, and streaming or downloading video was practically impossible. In addition, accounts (such as email) were limited in the amount of storage provided – no one could, for free, store terabytes of data in the cloud as they can today.

In addition, locating material took time and effort. The search engines available today have progressed by leaps and bounds over what was available then. In the late 1990s, companies that provided world wide web “directories” actually reviewed material

³¹ 982 F. Supp. 503 at 514.

as they catalogued it, rather than sending automated “robots” to crawl everything online with blazing speed.³²

On the other side of the coin, copyright owners had relatively few automated tools at their disposal to detect infringements. Specialized vendors to crawl the Web and flag infringing files were beginning to emerge, but their methods were relatively primitive.

Attracting advertising to a website or service also required greater effort. Whereas now ad servers like Google run targeted ads on millions of websites through embedded links, in the late 1990s, a website who wanted to generate funds from infringing conduct had to charge subscription prices or actually solicit advertisers. Similarly, a user who wanted to find infringing content would not see ads for such content displayed alongside search results after Googling for a recording artist by name. Today, according to our research, users are connected to infringing content through search engines more so than through any other means.³³

Peer-to-peer file sharing did not yet exist, at least in a manner accessible to most people. In fact, many of the services that possess large market share online now, were in their infancy or did not yet exist at the time the DMCA was enacted. For example, Facebook, Instagram, Twitter, iTunes, Spotify, YouTube, PayPal and Skype did not exist. eBay, Amazon, Google, and Yahoo! were all less than 5 years old.

ii. Legislative History of the DMCA

While the cases discussed above were reaching resolution, the United States signed the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty. These treaties required certain changes to U.S. law, including protection for technological protection measures used to prevent misuse of copyrighted works and copyright management information used to identify right holders. Although the treaties did not require any liability limitations for Internet service providers, it became a political reality that legislation to implement the treaties could not be passed without accommodating demands made by large providers such as America Online, Yahoo!, CompuServe and Verizon.³⁴

³² See Senate Judiciary Committee Report, S. Rep. No. 105-190, at 49 (1998) (“The Yahoo! directory, for example, currently categorizes over 800,000 online locations and serves as a “card catalogue” to the World Wide Web, which over 35,000,000 different users visit each month. Directories such as Yahoo!’s usually are created by people visiting sites to categorize them. It is precisely the human judgment and editorial discretion exercised by these cataloguers which makes directories valuable.”).

³³ In a survey of digital music listeners by consumer research firm MusicWatch, search engines were found to be one of the leading way to discover pirated music. Crupnick, *supra* n. 8. Another study from Carnegie Mellon University, perhaps the most comprehensive study yet on the link between search engines and media piracy, confirmed what search engines have likely known all along: that more highly placed links do have an effect influencing consumer behavior. The study showed that even users looking for lawful content could be led astray by promoted links to pirated content. Liron Sivan, Michael D. Smith, and Rahul Telang, *Do Search Engines Influence Media Piracy?: Evidence from a Randomized Field Study*, SCHOOL OF INFORMATION SYSTEMS AND MANAGEMENT, HEINZ COLLEGE, CARNEGIE MELLON UNIVERSITY (Sept. 12, 2014), <http://ssrn.com/abstract=2495591>.

³⁴ See Levine, *supra* n. 9.

In the House of Representatives, the implementing legislation (called the “WIPO Copyright Treaties Implementation and Online Copyright Infringement Liability Limitation Act”) contained language intended to “codify the core of current case law dealing with liability of online service providers.”³⁵ Under this bill, direct infringement could not be “based solely on the intermediate storage and transmission of material through a system or network” so long as specific circumstances existed. The legislation also included liability limitations for contributory and vicarious infringement for the actions described above as well as for otherwise “transmitting or providing access to material over the provider’s system or network,” so long as the provider lacked actual knowledge that material was infringing or awareness of facts and circumstances from which infringement was apparent and the provider did not receive a financial benefit directly attributable to the infringement where the provider had a right and ability to control the infringement.³⁶ The Report of the Judiciary Committee that accompanied the bill³⁷ explained the purpose of the provisions as follows:

As to direct infringement, liability is ruled out for passive, automatic acts engaged in through a technological process initiated by another. Thus, the bill essentially codifies the result in the leading and most thoughtful judicial decision to date: *Religious Technology Center v. Netcom On-line Communications Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995). In doing so, it overrules those aspects of *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993), insofar as that case suggests that such acts by service providers could constitute direct infringement, and provides certainty that *Netcom* and its progeny, so far only a few district court cases, will be the law of the land. As to secondary liability, the bill changes existing law in two primary respects: (1) no monetary relief can be assessed for the passive, automatic acts identified in *Religious Technology Center v. Netcom On-line Communications Services, Inc.*; and (2) the current criteria for finding contributory infringement or vicarious liability are made clearer and somewhat more difficult to satisfy.³⁸

The House bill was also the source of the “red flag” test found in the enacted legislation, as part of an overall effort to “[m]odif[y] and clarify[y] the knowledge element of contributory infringement and the financial benefit element of vicarious liability. . . . The knowledge standard in subparagraph (A), in addition to actual knowledge, includes ‘facts or circumstances from which infringing activity is apparent.’ This would include a notice or any other ‘red flag’—information of any kind that a reasonable person would rely upon. It may, in appropriate circumstances include the absence of customary indicia of ownership or authorization, such as a standard and accepted digital watermark or other copyright management information. As subsection (b) makes clear, the bill imposes no obligation on a provider to seek out such red flags.

³⁵ H.R. Rep. No. 105-551.

³⁶ See Irina Y. Dmitrieva, *I Know It When I See It*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 233 (2000) (chronicling development of legislation); *House Judiciary Approves Copyright Reform For Digital Environment*, 55 Pat. Trademark & Copyright J. (BNA) 519 (Apr. 2, 1998); *Industry Groups Reach Accord on Online Copyright Liability Limitation*, 55 Pat. Trademark & Copyright J. (BNA) 557 (Apr. 9, 1998).

³⁷ House Judiciary Committee Report, H.R. Rep. No. 105-551.

³⁸ *Id.*

Once a provider becomes aware of a red flag, however, it ceases to qualify for the exemption. This standard differs from existing law, under which a defendant may be liable for contributory infringement if it knows or should have known that material was infringing.”³⁹

Ultimately, Congress did not follow the approach of directly codifying the Netcom liability standards. Instead, beginning with the Senate bill, the legislation created “safe harbors” within which service providers who were liable for direct or secondary infringement “by reason of” engaging in four specified categories of activity were immunized against all monetary liability and much injunctive relief, if they met certain conditions.⁴⁰ The Report explained the overall purpose and scope of the liability limitations as follows:

Although the copyright infringement liability of on-line and Internet service providers (OSPs and ISPs) is not expressly addressed in the actual provisions of the WIPO treaties, the Committee is sympathetic to the desire of such service providers to see the law clarified in this area. There have been several cases relevant to service provider liability for copyright infringement. Most have approached the issue from the standpoint of contributory and vicarious liability. Rather than embarking upon a wholesale clarification of these doctrines, the Committee decided to *leave current law in its evolving state* and, instead, to create a series of ‘safe harbors,’ for certain common activities of service providers. A service provider which qualifies for a safe harbor, receives the benefit of limited liability. ... Title II preserves strong incentives for service providers and copyright owners to *cooperate to detect and deal with copyright infringements that take place in the digital networked environment*. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.⁴¹

The “common activities of service providers” eligible for safe harbor treatment were: (1) “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or the intermediate and transient storage of such material in the course of such transmitting, routing or providing connections”; (2) “intermediate and temporary storage of material on the system or network controlled or operated by for the service provider [where another person initiates the presence of the material and] ... where the storage is carried out through an automatic technical process for the purpose of making such material available to users of such system or network...”; (3) storage at the direct of a user of material that resides on a system or network controlled or operated by of for the service provider”; and (4) “referring or linking users to an online location containing infringing material or activity by using information location tools, including a directory, index, reference,

³⁹ *Id.*

⁴⁰ An earlier bill introduced by Senator Ashcroft contained broader immunity for service providers. *See Liability Bill for Online Service Providers Focuses on Notice and Take Down, Fair Use, 54 Pat. Trademark & Copyright J. (BNA) 384 (Sept. 11, 1997).*

⁴¹ Senate Judiciary Committee Report, S. Rep. No. 105-190.

pointer or hypertext link”.⁴² Limitations (2) through (4) were limited to circumstances where the provider responded “expeditiously” to “notifications of claimed infringement” from copyright owners (a so-called “notice-and-takedown process”), and, similar to the House bill, lacked actual knowledge that material was infringing or awareness of facts and circumstances from which the infringement was apparent, and did not receive a direct financial benefit directly attributable to infringing activity that the service provider had a right and ability to control.⁴³

With respect to the knowledge related limitations on the liability limitations, the Senate Judiciary Committee Report that accompanied the legislation⁴⁴ clarified that the “intended objective” of the “red flag” knowledge standard referred to by the House Judiciary Report was “to exclude sophisticated ‘pirate’ directories—which refer Internet users to other selected Internet sites where pirate software, books, movies, and music can be downloaded or transmitted—from the safe harbor.”⁴⁵ Such pirate directories refer Internet users to sites that are obviously infringing because they typically use words such as ‘pirate,’ ‘bootleg,’ or slang terms in their uniform resource locator (URL) and header information to make their illegal purpose obvious to the pirate directories and other Internet users.”⁴⁶ The Report also provided this example: “For instance, the copyright owner could show that the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly, at the time the directory provider viewed it, a ‘pirate’ site of the type described below, where sound recordings, software, movies or books were available for unauthorized downloading, public performance or public display.”⁴⁷ The Report also states: “The ‘red flag’ test has both a subjective and an objective element. In determining whether the service provider was aware of a ‘red flag,’ the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a ‘red flag’ – in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances – an objective standard should be used.”⁴⁸

Regarding the financial benefit limitation on the liability limitations, the Report stated:

In determining whether the financial benefit criterion is satisfied, courts should take a common-sense, fact-based approach, not a formalistic one. In general, a service provider conducting a legitimate business would not be considered to receive a “financial benefit directly attributable to the infringing activity” where the infringer makes the same kind of payment as non-infringing users of

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

the provider's service. Thus, receiving a one-time set-up fee and flat periodic payments for service from a person engaging in infringing activities would not constitute receiving a "financial benefit directly attributable to the infringing activity." Nor is subparagraph (B) intended to cover fees based on the length of the message (per number of bytes, for example) or by connect time. It would however, include any such fees where the value of the service lies in providing access to infringing material.⁴⁹

The Report also clearly stated that "Section 512 does not require use of the notice-and-takedown procedure. A service provider wishing to benefit from the limitation on liability under subsection (c) must 'take down' or disable access to infringing material residing on its system or network of which it has actual knowledge or that meets the 'red flag' test, even if the copyright owner or its agent does not notify it of a claimed infringement. For their part, copyright owners are not obligated to give notification of claimed infringement in order to enforce their rights."⁵⁰

The Senate bill also included two additional prerequisite for safe harbor status, neither of which were contained in the House bill. The bill required a service provider to adopt and reasonably implement "a policy for the termination of subscribers of the service who are repeat infringers" and to accommodate and not interfere with "standard technical measures ... used by copyright owners to identify or protect copyrighted works [] that have been developed pursuant to a broad consensus of copyright owners and service providers..."⁵¹

The Senate Judiciary Committee Report said the following about these requirements:

First, the service provider is expected to adopt and reasonably implement a policy for the termination in appropriate circumstances of the accounts of subscribers of the provider's service who are repeat online infringers of copyright. The Committee recognizes that there are different degrees of online copyright infringement, from the inadvertent to the noncommercial, to the willful and commercial. In addition, the Committee does not intend this provision to undermine the principles of subsection (l) or the knowledge standard of subsection (c) by suggesting that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing. However, those who repeatedly or flagrantly abuse their access to the

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ 17 U.S.C. §§ 512(i).

Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access. Second, a provider's system must accommodate, and not interfere with, standard technical measures used to identify or protect copyrighted works. The Committee believes that technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age. For that reason, we have included subsection (h)(1)(B), which is intended to encourage appropriate technological solutions to protect copyrighted works. The Committee strongly urges all of the affected parties expeditiously to commence voluntary, interindustry discussions to agree upon and implement the best technological solutions available to achieve these goals. Subsection (h)(1)(B) is explicitly limited to "standard technical measures" that have been developed pursuant to a broad consensus of both copyright owners and service providers in an open, fair, voluntary, multi-industry standards process. The Committee anticipates that these provisions could be developed both in recognized open standards bodies or in ad hoc groups, as long as the process used is open, fair, voluntary, and multi-industry and the measures developed otherwise conform to the requirements of the definition of standard technical measures set forth in paragraph (h)(2). A number of recognized open standards bodies have substantial experience with Internet issues. The Committee also notes that an ad hoc approach has been successful in developing standards in other contexts, such as the process that has developed copy protection technology for use in connection with DVD.⁵²

Similar to the House bill, the Senate bill also contained a provision that stated that nothing in the legislation "should be construed to condition the applicability" of the liability limitations "on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity."⁵³ However, the Senate bill qualified this provision to account for the expected development of the standard technical measures discussed above, which could require monitoring by service providers.⁵⁴ The Report explained the "no monitoring" provision was "designed to protect the privacy of Internet users."⁵⁵

Once the House Commerce Committee amended the House bill to include the liability limitations of the Senate bill, the Commerce Committee issued another Report on

⁵² Senate Judiciary Committee Report, S. Rep. No. 105-190.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *Id.*

the legislation.⁵⁶ This Report largely parrots the language quoted above from the Senate Judiciary Report. The final Conference Report issued by the House and Senate said very little about the liability limitations.⁵⁷ However, both of these later reports emphasized that the legislation was intended to protect copyright owners in the Internet environment. Both Reports state: “Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.”⁵⁸ The Conference Report also states that “this legislation is not intended to discourage the service provider from monitoring its service for infringing material.”⁵⁹

⁵⁶ House Commerce Committee Report, H.R. Rep. No. 105-551, pt. 2 (1998).

⁵⁷ Conference Report on H.R. 2281, the Digital Millennium Copyright Act, H.R. Rep. No. 105-796 (1998).

⁵⁸ *Id.*

⁵⁹ *Id.*

Appendix C

Music Community Written Submission
October 16, 2015

Regarding Development of the Joint Strategic Plan on Intellectual Property Enforcement, in response to Request of the U.S. Intellectual Property Enforcement Coordinator for Public Comments, 80 Fed. Reg. 52800 (September 1, 2015)

The submitting parties (the “Music Community”), described in Appendix A hereto, are associations and organizations whose members create and disseminate a wide variety of copyrighted musical compositions and sound recordings. The Music Community has fully embraced the Internet marketplace as the primary avenue for delivering high-quality content to fans of music through a variety of exciting platforms. Collectively, the Music Community represents hundreds of thousands of songwriters, composers, music publishers, recording artists, record labels, studio professionals, and others, who rely on copyright protection for their livelihoods.

I. Introduction

The Music Community sees itself as a key contributor and participant in the digital marketplace. Music can be experienced in a rapidly increasing variety of ways through an ever-evolving choice of innovative platforms that are in high demand. As a result, musicians, songwriters, music publishers, record labels, consumers, device manufacturers, online music distributors, website providers, app developers and Internet access providers are all benefitting.

However, significant challenges remain. Copyright theft continues to proliferate online, despite the widespread availability of affordable, lawful content. Thus, the Music Community strongly believes that it is crucial for the Office of the IPEC to continue to play a positive role in strengthening and ensuring the appropriate balance for our copyright system for the digital age. This can be achieved in a variety of ways, including via government involvement in coordinating voluntary best practices initiatives, as well as legislative reform and regulatory actions.

For example, the enforcement mechanism and eligibility tests for the safe harbors in the Digital Millennium Copyright Act (“DMCA”) must be improved. Since passage of the DMCA, the digital landscape and the music industry have dramatically changed. Initially the DMCA was primarily designed to prevent isolated infringement by third parties on specific online sites when connection speeds were slower than today and storage space was limited. In that environment, these third parties were not able to infringe on the massive scale that they do today, and the “takedown notice” provisions were thought to provide an alternative to lengthy and expensive legal proceedings. The qualification standards for the safe harbor eligibility were thought to be available only to innocently infringing ISPs with no connection to the third party content they hosted, linked to or otherwise transmitted. The notice and take down process was intended as a safeguard to provide a mechanism for copyright owners to prevent infringement by even innocent ISPs.

But in the transformed Internet environment of today, as online speeds have dramatically increased while the cost of storage space has dramatically decreased, the DMCA’s failure to

scale has rendered it increasingly obsolete and futile from an enforcement standpoint. Large, sophisticated entertainment-oriented websites have developed, and they premise their business models on being shielded from responsibility by the safe harbors. Instead of sending a relatively small number of “take-down” notices to prevent isolated infringement in a manner that ensures the material doesn’t reappear, the Music Community is instead faced with the unprecedented burden of attempting to “take-down” literally billions of infringing copies of music and associated links from thousands of unauthorized sources in an environment where infringers feel free to simply continuously repost links to the infringing content. This mismatch between the amount of infringement and the burden of enforcement has increasingly led to the devaluation of music and the perception that there is no effective remedy against unauthorized infringement. Once a song is available, authorized or not, the law provides no means to effectively protect the Music Community’s property. Adding insult to injury, some ISPs have complained about “abusive DMCA notices” – they seek to curtail one of the only remedies left for copyright owners.

In sum, after 15 years of case law and changes in the marketplace noted above, the safe harbors can no longer be said to balance the burdens of policing copyright infringement between the ISPs and the owners. Consider that since the creative community’s last submission to the Intellectual Property Enforcement Coordinator (IPEC) in August, 2012 (the 2012 IPEC Submission),¹ the Recording Industry Association of America (RIAA) has sent over 128 million infringement notices in the aggregate to web site operators, their underlying hosting providers, and search engines. Unfortunately, all too often, when a work is “taken-down” on a particular site or in a search engine index, it immediately re-appears someplace else on that site, or on mirror sites. Congress never intended for things to work in this way. The extent of this “whack-a-mole” problem was not anticipated and, unfortunately, this DMCA loophole has been embraced as a way to continually use and profit from unauthorized use of music, and still arguably maintain the “safe-harbor” protections built into the DMCA, at least until a costly and time consuming lawsuit is filed and won.²

The Music Community stands willing to monitor for infringement and to do its best to cooperate to limit its impact. Self-help against pirate sites is certainly an action available to copyright owners, but without cooperative partners it has limited utility. And, generally, the

¹ Joint Submission of MPAA, NMPA, and RIAA to Office of the Intellectual Property Enforcement Coordinator 7-13 (Aug. 10, 2012), <http://www.regulations.gov/#!documentDetail;D=OMB-2012-0004-0248> [hereinafter 2012 IPEC Submission].

² It must be noted that what is expensive and difficult for large copyright owners is an impossible challenge for small copyright owners seeking to protect the value of their works from indiscriminate sharing online. As Maria Schneider, a three-time GRAMMY winning jazz and classical composer, bandleader and conductor noted in describing the frustration with the DMCA, “[t]he DMCA makes it my responsibility to police the entire Internet on a daily basis. As fast as I take my music down, it reappears again on the same site—an endless whack-a-mole game.” See *Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intell. Prop. and the Internet of the H. Comm on the Judiciary*, 113th Cong. 57 (2014) (statement of Maria Schneider).

courts have not been helpful in this regard. Recent judicial decisions have interpreted the DMCA in a way that puts an unfair burden on the copyright owner, while allowing the online services to use the “safe harbor” provisions in the law more as a sword than as a shield. Moreover, litigation against sites that provide pirated content has proven a long and costly process.³ And it simply doesn’t scale when there are thousands of sites that are dedicated to music theft.

This also places an undue burden on the literally hundreds of licensed sites in the United States. These services have acknowledged the moral and legal responsibility to pay for music yet they, like the copyright owners, are forced to compete with illicit businesses offering stolen versions for “free.”

The submitting parties, representing a vast cross-section of authors and owners of music, believe the IPEC can play a positive role in promoting reform of the enforcement mechanism of the DMCA and other aspects of the Copyright Act. It can also do much to advance the proposition that reducing the availability of infringing content online should be the shared goal of all legitimate businesses that operate online, as well as of consumers and the U.S. government. Whether by facilitating legislative reform, or helping to develop voluntary industry-wide best practices, the IPEC can help restore the rights of those who have been profoundly harmed as the scope and volume of the online infringement problem has rushed far beyond the ability of the DMCA framework to scale.

II. Current Trends in the Music Industry

A. Strong Public Demand for Music Fuels the Success of the Internet and the Consumer Electronics Industry

Demand for music online is higher than ever, with many sites directly dependent upon professionally produced, copyrighted music for their success. Over 65% of Americans ages 13+ agree that music is important to their lifestyle.⁴ American consumers spend, on average, more than 24 hours per week listening to music and, in a typical week, 75% of U.S. consumers listen to music online.⁵ Twelve of the top 20 most followed people on Twitter are from the Music Community.⁶ Fifteen of the top 20 celebrities on Facebook are musicians.⁷

³ For example, it took over five years of litigation for the record labels to prevail in their litigation against LimeWire, which had spent the better part of a decade inducing – and profiting from – peer-to-peer pirating of sound recordings. *See* Arista Records, LLC et al. v. Lime Group LLC, et al., 784 F. Supp. 2d 398 (S.D.N.Y. 2011).

⁴ Source: MusicWatch Inc., 2014 Annual Music Study.

⁵ *Music is Still the Soundtrack to our Lives*, Nielsen (Sept. 14, 2015), <http://www.nielsen.com/us/en/insights/news/2015/music-is-still-the-soundtrack-to-our-lives.html>.

⁶ Twitter Top 100 Most Followers, Twitter Counter, <http://twittercounter.com/pages/100> (last visited Oct. 2, 2015).

Since the last IPEC Joint Strategic Plan on Intellectual Property Enforcement, legitimate online services that enable people to listen to and interact with music have continued to proliferate and become more viable business models.⁸ Consumers have never had so many choices for experiencing music legitimately and instantaneously. However, for these services to have continued success, strong protection of copyright is required, as many unauthorized disseminators of music undermine the value of the legitimate sites.

In addition to physical formats for music, some of the exciting services available today include the following, with most offered on both wireline and mobile platforms:⁹

- Music is available for download through services like iTunes, AmazonMP3, eMusic, GhostTunes, 7digital, Google Play and several others, including in formats that allow consumers access across multiple devices for personal use without interoperability problems.
- Higher resolution music downloads, for greater fidelity, are available from services such as Pono, HD Tracks, Presto Classical and Pro Studio Masters.
- Interactive, on-demand music streaming services such as Rhapsody, Apple Music, Spotify, Deezer and Rdio offer unlimited listening – on computers or smart phones – for modest monthly fees. They also offer to subscribers the ability to listen off-line.
- Free ad-supported, audio-visual streaming sites, such as YouTube and Vevo, offer free streaming of music videos.
- Digital radio services, such as iHeartRadio, iTunes radio, and Sirius/XM, are available for free with limited advertising support or, in some cases, on a subscription basis.
- Over 750 different AM/FM stations are available as digital radio simulcasts.
- Licensed lyrics sites enable music lovers to access the lyrics to their favorite songs with the click of a mouse and to comment on those lyrics and learn about the songwriters and recording artists.
- Licensed apps like Flipagram enable consumers to interact with music like never before by creating photo and video stories set to music.

Due to all of this innovation, in the first half of 2015, digital dissemination accounted for 76% of the overall recorded music market by value, compared with 59% for 2012.¹⁰ In the U.S.,

⁷ Top Celebrities on Facebook, Fan Page List, <http://fanpagelist.com/category/celebrities/> (last visited Oct. 11, 2015). See also *Music Fuels the Internet*, an RIAA site that notes the top accounts on social media on a daily basis: <http://www.musicfuels.com/>.

⁸ See Cary Sherman, *Valuing Music in A Digital World*, Forbes (Sept. 23, 2015), <http://www.forbes.com/sites/realspin/2015/09/23/how-government-set-licensing-killed-the-music-industry/>.

⁹ See www.whymusicmatters.com for a variety of other licensed music services available in the United States, and www.pro-music.org for a worldwide listing.

digital subscription revenues increased in 2014, as sales of smartphones and tablets that promote use of streaming services increased streaming revenues sharply (in some cases, substituting for downloads).¹¹ In the first half of 2015, U.S. revenues from digital paid subscriptions were \$478 million, up 25% from the previous year.¹²

B. There is an Unacceptable Value Gap between the Demand for Music and the Revenue Returned to the Authors and Owners of that Music

Despite music being more popular than ever today, music industry revenues have been nearly flat since 2010, and are less than half what they were in 2000 (adjusted for inflation). Why is that?

The fact is that while the technology industry is benefitting from the increased availability of online music, and profiting from the unprecedented consumption and interest in music, the Music Community is facing a value gap. “When vinyl records, which peaked in the 1960s and ’70s, generate more revenue for the industry in 2014 than the billions of ad-supported on-demand streams on YouTube and similar services, something is fundamentally wrong with the market.”¹³ In short, music adds significant value to technologies and network access, but the Music Community is not receiving a fair share of the revenue.¹⁴

The broken state of the law, particularly the DMCA (discussed in more detail below), is playing a significant role in perpetuating this unfairness.¹⁵ The laws that “were designed to exempt passive intermediaries from liability,” the so-called safe-harbors, should never have been allowed to “exempt active digital music services from having to fairly negotiate” licenses with rights holders.¹⁶ Not only do certain actors take advantage of these safe harbors to profit from music without compensation to the authors and owners of that music, this situation unfairly

¹⁰ See Joshua P. Friedlander, *News and Notes on 2015 Mid-Year RIAA Shipment and Revenue Statistics 1* (Sept. 22, 2015), <http://riaa.com/media/238E8AC7-3810-A95C-44DC-B6DEB46A3C6E.pdf> [hereinafter *RIAA Shipment and Revenue Statistics*].

¹¹ IFPI Digital Music Report 2015, 7-8, <http://www.ifpi.org/downloads/Digital-Music-Report-2015.pdf>.

¹² See *RIAA Shipment and Revenue Statistics*, *supra* n. 10, at 2.

¹³ See Sherman, *supra* n. 8.

¹⁴ See David Israelite, *NMPA Head Says “Free” May Work For Pandora But is Devastating to Songwriters: Op-Ed*, *Billboard* (Sept. 24, 2015), <http://www.billboard.com/articles/business/6707834/nmpa-david-israelite-oped-pandora-songwriter-payments>.

¹⁵ See Sherman, *supra* n. 8. The flawed U.S. music licensing regime also plays a factor in this value gap. See Israelite, *supra* n. 14.

¹⁶ See Frances Moore, *Artist and Record Companies need a Fair Digital Marketplace* (July 29, 2015), <http://www.ifpi.org/news/Artists-and-Record-Companies-Need-A-Fair-Digital-Marketplace>.

distorts the market value for music, creating below-market discounted rates that harm the entire music industry. It cannot be right, for example, that, by some accounts, YouTube has 40% of the music listening but only provides 4% of the revenue to the record labels.¹⁷ As the CEO of RIAA noted, the Music Community is faced with a “Hobson’s choice: Accept below-market deals or play that game of whack-a-mole. The notice and takedown system—intended as a reasonable enforcement mechanism—has instead been subverted into a discount licensing system where copyright owners and artists are paid far less than their creativity is worth.”¹⁸

To turn the digital transformation of the music industry into sustainable long-term growth, this value gap must be addressed. A successful Music Community that invests in music and rewards creators needs a balanced digital marketplace in which to negotiate terms for the use of its music. And, as further discussed below, it needs a balanced and fair legal enforcement system in which to operate to do so.

III. Online Theft Persists Via an Ever-Evolving Variety of Platforms

A. Music Theft Online Continues to Persist and Harm the Music Community and the U.S. Economy

Though there are more legitimate options than ever for downloading, streaming and interacting with music, online piracy remains a large threat to the Music Community. Since the last IPEC submission, RIAA has monitored 2,159 sites, and noticed 48,391,597 infringements directly to sites. This is in addition to millions of notices sent to ISPs hosting those sites and the search engines indexing and directing traffic to those sites.

This piracy affects the U.S. labor market, and has led to a decline in the number of people employed by the music industry. “The music industry, while enormous in its economic, cultural and personal impact, is by business standards relatively small. So theft on this scale has a noticeable and devastating impact: employment at the major U.S. music companies has declined by thousands of workers, and artist rosters have been significantly cut back. The successful partnership between a music label and a global superstar – and the revenue generated – finances the investment in discovering, developing and promoting the next new artist. Without that revolving door of investment and revenue, the ability to bring the next generation of artists to the marketplace is diminished – as is the incentive for the aspiring artist to make music a full time professional career.”¹⁹ Such piracy hurts not only the large music companies or employees of

¹⁷ See video, *HBOs Richard Plepler and Jimmy Iovine on Dreaming and Streaming from the Vanity Fair Summit*, Vanity Fair (Oct. 8, 2015), <https://www.youtube.com/watch?v=HoODO8HkvoI>; Kia Makarechi, Twitter Posting (Oct. 7, 2015, 1:25pm), https://twitter.com/kia_mak/status/651855850840195078?refsrc=email&s=11.

¹⁸ See Sherman, *supra* n. 9.

¹⁹ See *Piracy Online: Scope of the Problem*, RIAA, https://www.riaa.com/physicalpiracy.php?content_selector=piracy-online-scope-of-the-problem, (last visited Oct. 9, 2015) [hereinafter *Scope of the Problem*].

those companies – independent creators are harmed as well. The Nashville Songwriters Association International reports that, since 2000 (essentially, in the post-Napster era), the number of full-time songwriters in Nashville has declined by 80%.²⁰ In the end, consumers and legitimate technology companies also suffer, because incentives for music production decline, lawful services are forced to square off against unfair competition, and the drivers of the Internet’s success are threatened.

B. Current Forms of Music Theft Online

Three years ago, the creative industries highlighted in the 2012 IPEC Submission that online theft continued unabated. Although much has changed in the last three years, much has stayed the same. The same forms of piracy that existed three years ago, from unauthorized streaming and download sites, to cyberlockers, peer-to-peer networks, and mobile apps, continue to proliferate at unacceptable levels today.²¹ Others, such as stream-ripping, which existed three years ago, have gained increased popularity in the past year, as more and more users turn to this form of piracy to download music to their devices. In the last three years we have also seen escalating damage from the unauthorized dissemination of pre-release music, *i.e.*, albums slated for commercial release that have not yet been commercially released to the public.²²

Some of the piracy problems the Music Community is encountering include:

- **Mobile Applications:** Infringing mobile applications provide unauthorized streaming, downloading, stream-ripping, syncing to other videos or photographs, and/or distribution of music. Despite the industry’s efforts to have these infringing apps taken down from the leading mobile app storefronts,²³ they nonetheless continue to proliferate. For example, in 2014, “the most popular of these Android apps, Music Maniac, ha[d] been downloaded more than 10 million times – and afford[ed] free access to all 10 of the top songs listed on the current Billboard’s Hot 100 list.”²⁴ In addition, live video streaming

²⁰ See Nate Rau, *Nashville’s Musical Middle Class Collapses* (Jan. 28, 2015), <http://www.tennessean.com/story/entertainment/music/2015/01/04/nashville-musical-middle-class-collapses-new-dylans/21236245/>.

²¹ For a detailed overview of various forms of piracy, see 2012 IPEC Submission, *supra* n. 1. Websites for the sale of physical counterfeits also remain a problem.

²² For example, ShareBeast, a cyberlocker that caused significant damage to the industry, trafficked in pre-release music, and boasted millions of users, was recently shut down by the Department of Justice. Andre Yoskowitz, *FBI Takes Down Pre-Release Music Piracy Site Share Beast*, News By AfterDawn, (Sept. 16, 2015), <http://www.afterdawn.com/news/article.cfm/2015/09/16/fbi-takes-down-pre-release-music-piracy-site-sharebeast>.

²³ To date, RIAA has noticed over 5,700 mobile apps to the major mobile app storefronts.

²⁴ Dawn Chmielewski, *Music Piracy Goes Mobile*, Re/Code, Mar. 24, 2014, <http://recode.net/2014/03/24/music-piracy-goes-mobile/>. Though Music Maniac is no longer available through Google Play, it remains available through other websites.

apps owned by Twitter and Facebook have led to unauthorized streaming of concerts by new and leading artists. Unfortunately, even when the Music Community has some success in inhibiting the reach of an unlicensed, infringing app, a new one takes its place, or the app developers find new avenues to distribute the app. For example, in December 2014, Google removed from its Play Store several clearly infringing applications associated with the notorious Pirate Bay website.²⁵ However, the apps remain available elsewhere and usable with Android devices. Moreover, all the apps downloaded prior to the takedown of the app from the storefront continue to function.²⁶

- Unauthorized Streaming and Download Services, Including Sites that Cater to Pre-release Music: This class of digital sites and apps directly or indirectly offers unauthorized on-demand streaming and/or downloading of our members' music, including their most popular and valuable content. They often provide not just one link to a particular track, but instead several pages of links to the same track, and/or have several more "URLs" with the same track "at the ready" to post to their site when another URL to the same track is noticed.²⁷ Several of these sites go further, providing unauthorized downloading of pre-release music.²⁸ Some are so brazen as to publicly tout their infringing activity and seek crowd sourcing to fund their illegal efforts.²⁹ Such infringing activity clearly

²⁵ Angela Moscaritolo, *Pirate Bay Apps Yanked from Google Play*, PC Magazine (Dec. 8, 2014) <http://www.pcmag.com/article2/0,2817,2473253,00.asp>.

²⁶ For example, while the Pirate Bay Browser App was removed from the Google Play store in June 2013, nearly a year later, in May 2014, there were an estimated 500,000+ monthly U.S. users of the app. *Source*: RIAA analysis of Mobidia data.

²⁷ *See* Capitol Records, LLC v. Escape Media Group, Inc., 2015 U.S. Dist. LEXIS 38007, *18-19 (S.D.N.Y. Mar. 25, 2015) (characterizing the infringing service Grooveshark as a "technological Pez dispenser" that required copyright owners to send "successive takedown notices" in order to remove a single song from the service).

²⁸ Leaks of pre-release music have long plagued the Music Community. *See* Stephen Witt, *The Man Who Broke the Music Business* (Apr. 27, 2015), <http://www.newyorker.com/magazine/2015/04/27/the-man-who-broke-the-music-business>. But with so many devices and unauthorized services at consumers' fingertips, unlawful releases of albums before they hit the legitimate marketplace can be devastating.

²⁹ A particularly egregious example is the new service Aurous, which allows users to search for, stream, and download pirated copies of popular music, and which is designed specifically to search for and retrieve copies from online sources notorious for offering pirated music. Aurous has promoted itself by linking to articles that call it "BitTorrent Music for Your Dad," and "Popcorn Time for Music"; in other words, as a site that makes it incredibly easy to find and stream or download pirated music. Aurous brazenly began a crowdfunding campaign for its mobile app, which it has since shut down. *See* Aurous, Twitter Posting (Sept. 17, 2015, 11:55am), <https://twitter.com/aurousapp/status/644585368440938496?lang=en> ("We need your help to bring Aurous to Iphone, Android and Windows phone! Please consider donating to our Indiegogo..."); Aurous, Twitter Posting (Sept. 19, 2015, 1:00pm), <https://twitter.com/aurousapp/status/645326516600086528?lang=en>. The RIAA, on behalf of its members, has brought suit against Aurous, seeking injunctive relief against this blatant infringer,

harms U.S. artists, songwriters, record labels and music publishers by disseminating their work without authorization and severely diminishing the commercial value of those works.

- Cyberlockers: While significant efforts have been invested in shutting down some of the worst actors in this space, such as Megaupload, ShareBeast, and RockDizFile, numerous websites still exist that are designed to encourage their users to post and disseminate infringing copies of music.³⁰ These sites become repositories for free access to professionally produced, copyrighted content.
- Peer-to-peer Networks: While 8.1 million people pay for streaming subscriptions in the United States, more than twice that many are still using peer-to-peer piracy sites for illegal downloads.³¹ And while use of peer-to-peer sites may not be rising as quickly during recent years as it once did, the harm that the availability of infringing copies on those networks presents remains devastating.
- Unauthorized Lyrics Sites: Sites that provide unauthorized access to reproduced song lyrics also present a real problem for music publishers and songwriters. There are so many of these websites, with associated applications, that National Music Publishers' Association (NMPA) was forced to initiate a litigation campaign to compel those sites that wanted to avoid injunctions and liability to obtain licenses.³² Although this approach had some success, myriad infringing sites and apps remain available, supported by advertising.
- Stream Ripping: Finally, some companies are profiting from enabling consumers to exceed their authorized access to lawful products, such as YouTube and audio-only streaming services, by creating "ripped" illegal copies of streams. This is particularly damaging because it prevents copyright owners from obtaining full value from licensors who offer purchases of permanent copies of works.

and the court granted a temporary restraining order against Aurous on October 15, 2015. *See* Atlantic Recording Corporation et al. v. Andrew Sampson, Case No. 1:15-cv-23810 (S.D. Fla., filed Oct. 13, 2015); Temporary Restraining Order, *id.* (Oct. 15, 2015).

³⁰ For examples of such cyberlockers, see the RIAA Notorious Market Submission Report (Oct. 5, 2015), <http://riaa.com/media/9F859538-E1E1-CC7E-A701-84F9FB3851BF.pdf> [*hereinafter* RIAA NMR Submission].

³¹ Ryan Faughnder, *Music Piracy is Down But Still Very Much in Play*, Los Angeles Times (June 28, 2015), <http://www.latimes.com/business/la-et-ct-state-of-stealing-music-20150620-story.html>.

³² *See* Ed Christman, *NMPA Launches Suits Against Infringing Lyric Sites*, Billboardbiz (May 21, 2014), <http://www.billboard.com/biz/articles/news/publishing/6092270/nmpa-launches-suits-against-infringing-lyric-sites>; Ben Sisario, *In Music Piracy Battles, Lyrics Demand Respect Too*, New York Times (Nov. 11, 2013), http://www.nytimes.com/2013/11/12/business/media/in-music-piracy-battles-lyrics-demand-respect-too.html?_r=0.

A significant change from three years ago is the ability of rogue actors to engage in piratical activity across a variety of digital platforms, whether via computer software applications, web sites, plug-ins for Internet browsers, widgets for smart televisions, or mobile applications. Consider, for example, that before the infringing service GrooveShark was shuttered in light of a court order finding it liable for willful infringement, GrooveShark offered access to its service via a website, a mobile application, a browser plug-in, and was negotiating deals to have GrooveShark widgets on certain smart TVs.³³

In addition, it is now easier than ever for rogue operators to jump physical jurisdictions and digital domains, while obfuscating their path while they do so. The increasing ubiquity of high-bandwidth connectivity and technologically sophisticated hosting services in a growing number of offshore jurisdictions will make it increasingly easy for thieves to fully exploit the U.S. market while minimizing, for practical purposes, their exposure to U.S. copyright or criminal law. Another factor that will accelerate this disturbing trend in future years involves the domain name system. Beyond the existing framework of country code Top Level Domains (ccTLDs), the ongoing rollout of new generic Top Level Domain (gTLD) registries includes some based in jurisdictions more tolerant or even encouraging of theft of U.S. intellectual property. This gives pirates a wider range of havens to seek.

Consider that in 2014, rogue site Mp3Skull was at domain mp3skull.com, and hosted at a U.S. hosting company. Since then, Mp3Skull had moved to five different top level domains, with two changes in the last two weeks. As of October 11, 2015, Mp3Skull was located at mp3skull.wtf, and had moved its servers outside of the U.S.³⁴ It obfuscates its operators and location by using a privacy/proxy service to hide the operator and Cloudflare to hide its IP address.³⁵

This domain hopping, along with the steps such pirate sites take to obfuscate its identity and physical location, provide further obstacles to effective enforcement.

This highlights that as the landscape continues to shift under our feet at rapid speeds, it has become even harder to pin down where and how the next form of infringement will emerge, and what combination of jurisdictions – digital or physical – will be implicated.

³³ Consider also that rogue cyberlocker 4shared.com offers its service both via a website and a mobile application. See www.4shared.com, last visited October 11, 2015. Rogue stream-ripper FLVTO offers its infringing activity via a website and a computer application. See www.flvto.biz, last visited October 11, 2015.

³⁴ Another example, noted in the RIAA NMR Submission, is rogue site Viperial. Viperial, which was originally at viperial.com, then redirected to viperial.co, and now redirects to viperial.me. See also footnote 59 and Appendix B for further examples.

³⁵ See IP Tracker Lookup, “mp3skull.com”, <http://www.ip-tracker.org/locator/ip-lookup.php?ip=mp3skull.com>, last visited Oct. 12, 2015.

C. The Role of Third Parties in Supporting, Promoting, or Profiting from Copyright Theft

Numerous third parties, both legitimate actors and illegitimate, including some of those noted above, help to facilitate access to the infringing services discussed above, including domain name registrars and registries, search engines, app stores, hosting companies and content delivery networks (CDNs), advertisers, and payment processors. Regardless of whether the activities engaged in by such companies rise to the level of incurring liability under existing copyright laws, far more could and should be done by such third parties to help prevent and limit infringement.

Below is a brief description of the role some of these third parties play, and what efforts, if any, have been taken to curb infringement occurring or facilitated via their services.

- Registrars, Registries, and Privacy/Proxy Services: A domain name is often a key resource that enables sites dedicated to digital theft to be accessed by their customer base; and even though registrar, registry and privacy/proxy terms of service almost uniformly prohibit the use of domain name registrations for such activities, these provisions are rarely enforced. Cooperation of registrars, registries and privacy/proxy service providers with right holders often leaves much to be desired. This refusal to take action despite verifiable evidence of infringement, coupled with the unfettered expansion of new internet real estate for the infringers to use, further exacerbates the music infringement problem.
- Search Engines: Search engines continue to be a key driver for music discovery and a significant tool that leads traffic to infringing sites.³⁶ While recent efforts by search engines to demote sites for which they have received high volumes of infringement notices have made an impact,³⁷ over time these efforts are being shown to have limited

³⁶ In a survey of digital music listeners by consumer research firm MusicWatch, search engines were found to be one of the most common ways users discover sites to download music without paying. See Joshua P. Friedlander, *More Evidence Is In – Intermediaries Matter*, RIAA Music Notes Blog (Sept. 15, 2014), http://www.riaa.com/blog.php?content_selector=riaa-news-blog&blog_selector=Intermediaries-Matter&news_month_filter=9&news_year_filter=2014. Another study from Carnegie Mellon University, perhaps the most comprehensive study yet on the link between search engines and media piracy, confirmed what search engines have likely known all along: that more highly placed links do have an effect influencing consumer behavior. The study showed that even users looking for lawful content could be led astray by promoted links to pirated content. Liron Sivan, Michael D. Smith, and Rahul Telang, School of Information Systems and Management, Heinz College, Carnegie Mellon University, *Do Search Engines Influence Media Piracy?: Evidence from a Randomized Field Study* (Sept. 12, 2014), available at <http://ssrn.com/abstract=2495591>.

³⁷ See, e.g., Katherine Oyama, *Continued Progress on Fighting Piracy*, Google Public Policy Blog (Oct. 17, 2014), <http://googlepublicpolicy.blogspot.com/2014/10/continued-progress-on-fighting-piracy.html>.

utility. First, far too often search engine operators are slow to act, electing to allow infringement to continue unabated for too long before down-ranking a site. Second, as shown in Appendix B, sites that engage in domain hopping after being demoted quickly rise again in search results. Clearly, the system is broken when Google estimates it will receive around 350 million takedown notices this year,³⁸ including tens of millions from the Music Community, and the piracy problem continues to exist at its current levels. More effective tools are required to reduce the amount of traffic search engines send to known rogue operators.

- Hosting Companies, CDNs, and their ilk: Hosting Companies, CDNs, and companies that provide similar services vary in the levels of cooperation or obstacles they place in the face of evidence of infringement occurring on or via their systems. Some, like Cloudflare or WebZilla, refuse to terminate service with their customer despite receiving thousands of notices of infringement attributable to one of their subscribers' accounts. Other hosting companies appear to terminate service with their rogue customer after receiving repeated notices of infringement associated with that customer, but there is no consistency in the response to the rights holder or in the level of knowledge of repeat infringement that leads to termination or suspension of service.
- Advertisers and Ad Networks: Following pledges made in 2012,³⁹ many U.S. advertisers, ad agencies and ad networks have taken proactive steps to deter placing ads on sites that engage in copyright infringement. Many will also take action when notified that their ads or services were used to place ads on infringing sites. In addition, over the past several months, portions of this industry have created and adopted further programs to help improve the digital ecosystem, including the Trustworthy Accountability Group's Brand Integrity Program Against Piracy.⁴⁰ However, several other ad networks, both in the U.S. and abroad, continue to funnel ad dollars to infringing sites. Other advertisers, particularly those that advertise using pay-per-install potentially unwanted programs (PUPs), continue to prominently interact with infringing sites. Moreover, the rogue operators are getting more sophisticated, engaging in various forms of ad fraud, such as

³⁸ See Chris Castle, *What Is the Intention of Justice? Notice and Stay Down Is the Government's Responsibility*, Huffington Post (Oct. 1, 2015), <http://www.huffingtonpost.com/chris-castle/what-is-the-intention-of-b-8208768.html>.

³⁹ See ANA, 4A's Release Statement of Best Practices Addressing Online Piracy and Counterfeiting, Association of National Advertisers (May 3, 2012), <https://www.ana.net/content/show/id/23408>.

⁴⁰ See *Advertising Industry Launches Initiative to Protect Brands Against Piracy Websites*, TAG (Feb. 10, 2015), <https://www.tagtoday.net/advertising-industry-launches-initiative-to-protect-brands-against-piracy-websites/>. Indeed, Group M, a leading global media investment management group, has announced that it will require all of its partners to be DAAP validated in 2016. *GroupM Requires Partners to use TAG-Certified Anti-Piracy Services*, TAG (Sept. 23, 2015), <https://www.tagtoday.net/groupm-requires-partners-to-use-tag-certified-anti-piracy-services/>.

pop-unders or re-directs to phony webpages, to channel advertising dollars their way. More needs to be done to address this fraudulent behavior.

- Payment Processors: In 2011, after significant assistance from the Office of the IPEC, payment processors and credit card companies implemented a set of best practices to investigate complaints and stop processing transactions for sites that distribute counterfeit and pirated goods. As implemented, these best practices have led to a significant reduction in the use of premier credit card services for not only sites that directly charge for unauthorized music downloads or streams, but also those that attempt to hide their efforts by charging indirectly for unauthorized access to music.⁴¹ While rogue sites continue to find alternative payment methods to profit from their illegal enterprises, the adoption and implementation of these best practices is an example of what is possible when industries agree to adopt reasonable approaches to exercise their responsibility to help ensure that Internet-based transactions are lawful.
- App Stores: Recently, some leading digital storefronts, such as iTunes and Google Play, have made increased efforts to address and remove from their digital storefronts apps that facilitate music infringement. Nonetheless, too often, digital storefronts, whether for mobile applications, browser plug-ins, or more traditional software applications, continue to offer applications that obviously facilitate piracy. This includes apps that clearly advertise the availability of unlicensed music. These platforms should do more to help lawful applications succeed by limiting piracy before the infringing apps ever make it on their storefront.

All of these third parties gain some financial benefit from their interactions with the rogue operators, whether in the form of information or dollars, and each has an ability to deter the use of its services for such illegal activity. As noted in the 2012 IPEC Submission, where commercially reasonable measures can be taken to address predictable and identifiable harms enabled by the services these businesses offer, those measures should be made. This not only helps address the infringement problem, it also helps create a safer, more robust digital ecosystem.⁴²

⁴¹ RogueBlock, the initiative that grew out of an agreement of the leading credit card companies and payment processors to develop best practices to deny sites that engage in copyright theft or counterfeiting the economically essential services they provide, has terminated over 5,000 individual counterfeiter's merchant accounts, impacting over 200,000 websites. *See RogueBlock*, IACC, <http://www.iacc.org/online-initiatives/rogueblock> (last visited Oct. 10, 2015).

⁴² *See, e.g.*, RIAA Comments to NTIA in Response to the Request for Public Comment on Stakeholder Engagement on Cybersecurity in the Digital Ecosystem (May 27, 2015), http://www.ntia.doc.gov/files/ntia/riia_5-27-15.pdf (noting the correlation between malware and other cybersecurity threats with online infringement).

IV. The Law is Inadequate to Address these Problems

As was noted in the 2012 IPEC Submission, the overarching challenge for copyright owners is to find meaningful ways to enforce their rights. Today, as then, there is not enough money in the world to fund litigation against every significant pirate, even if copyright owners could find courts that could exercise jurisdiction over all of them. And the statute that the U.S. enacted in 1998 to facilitate inter-industry cooperation in enforcement against infringement in the digital environment, the Digital Millennium Copyright Act (DMCA), has failed to achieve its purpose.

When the notice and takedown provisions of the DMCA were enacted, Congress intended to “preserve the strong incentives for service providers and copyright owners to detect and deal with copyright infringements that take place in the digital networked environment.”⁴³ The legislation was not “intended to discourage the service provider from monitoring its service for infringing material.”⁴⁴ However, given the increased availability of higher broadband speeds and low-cost server space, coupled with the continued misinterpretation of the DMCA by the courts and those that want to take advantage of its safe harbors,⁴⁵ the DMCA regime fails to accomplish the balance sought by Congress.

As a consequence of these judicial decisions, rather than providing incentives for cooperation, the DMCA has provided incentives for Internet businesses to turn a blind eye to infringement, or even to build willful blindness into their business models.⁴⁶ In fact, the DMCA,

⁴³ Report of House Commerce Committee on H.R. 2281, the Digital Millennium Copyright Act, H.R. Rep. No. 105-51, pt. 2, 49 (1998).

⁴⁴ Conference Report on H.R. 2281, the Digital Millennium Copyright Act, H.R. Rep. No. 105-796, 73 (1998).

⁴⁵ See, e.g., *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009), *aff'd*, *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022 (9th Cir. 2011); *Viacom Int’l, Inc. v. Youtube, Inc.*, 940 F. Supp. 2d 110, 115 (S.D.N.Y. 2013); *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500 (S.D.N.Y. 2013), *reconsideration granted in part, reconsideration denied in part*, 972 F. Supp. 2d 537 (S.D.N.Y. 2013); *Lenz v. Universal Music Corp.*, No. 13-16106, 2015 U.S. App. LEXIS 16308 (9th Cir. Sept. 14, 2015).

⁴⁶ See Terry Hart, *Grooveshark is Done*, Copyhype (Oct. 1, 2014), <http://www.copyhype.com/2014/10/grooveshark-is-done/>. (Grooveshark instructed its employees to create user accounts and to upload infringing files to the site, knowing that the business “depended on the use of infringing content); see also William Hensley, *Copyright Infringement Pushin’: Google, YouTube, and Viacom Fight for Supremacy in the Neighborhood that may be Controlled by the DMCA’s Safe Harbor Provision*, 51 IDEA 607, 626 (2011) (“YouTube’s business model was designed to maximize the number of site viewers in order to increase advertising revenue to attract a buyer. To increase the number of viewers, they needed infringing material.”). The DMCA’s current provision providing that monitoring is not required was intended to apply to innocent ISPs who otherwise meet the statutory eligibility tests for the safe harbors – not to shield ISPs operating with full awareness of the widespread presence of infringing content and indeed active inducement of posting of such content.

as interpreted by some, creates a perverse incentive for Internet business to take actions to deter the appearance of monitoring, contrary to the diligence expected in nearly any other business environment.

Even while removing individual infringing links identified in takedown notices, services based on infringement can thrive financially and expect to enjoy near-complete immunity from liability. More and more rogue operators appear to specifically design and engineer their systems and processes to make the DMCA, as they interpret it, irrelevant and ineffective to their ongoing infringement. Essentially, these rogue operators have learned the weaknesses of the DMCA as it has been interpreted and implement their services to exploit those weaknesses. In short, the problems with the DMCA identified in the 2012 IPEC Submission continue unbounded. The time is now for action to address this continued inequity.

V. Recommendations

Much can be done to curb the problems identified above so that legitimate music offerings succeed, more new music is produced than ever before, and the Internet marketplace delivers to consumers the types of exciting new services they are flocking to in large numbers. Improvements can be made through voluntary initiatives, legislatively, and through continued enforcement efforts.

A. Voluntary Best Practices

In addition to legislative, enforcement, and regulatory approaches to address intellectual property enforcement (discussed below), the Office of the IPEC and the government should continue to encourage the development and implementation of voluntary best practices to help move toward a piracy-free, robust and innovative online ecosystem.

It is important that online intermediaries, not just right holders, fully engage in the fight against digital theft, because often the service providers possess information that rights holders cannot obtain or have difficulty locating. For example, YouTube's Content ID system now enables rights holders to limit infringing files, which are technologically matched via fingerprint-based content recognition technology, from being made available via YouTube.⁴⁷ Facebook also will be testing a matching technology that will allow creators to identify matches of their videos on Facebook across the site, allowing for easier removal of unauthorized repeat content.⁴⁸ These systems rely on information collected from right holders to allow the services to identify and block infringing files before the public gains access to them. Only the sites themselves can enable such preventative measures, because only they have instantaneous access to information regarding what is being uploaded to their services. If other services that allow user-posted content (such as distribution hub sites) adopted similarly robust tools, a large amount of unauthorized content could be automatically removed or blocked from the web.

⁴⁷ See *How Content ID Works*, YouTube Help, <https://support.google.com/youtube/answer/2797370?hl=en>, last visited Oct. 14, 2015.

⁴⁸ See *An Update on Video Management on Facebook*, Facebook Media (Aug. 27, 2015), <https://media.fb.com/2015/08/27/an-update-on-video-management-on-facebook/>.

Effective private-sector action is not only possible, it is in the best interest of all legitimate businesses and consumers. The Music Community firmly believes that reducing the availability of infringing content online should be the shared goal of all legitimate businesses that operate online, as well as of consumers and the U.S. government. If the U.S.-based Music Community is thriving and producing compelling content, Internet usage will increase, consumers will eagerly embrace new services, more advertisements will be viewed, more searches will be conducted, more consumers will have the opportunity to enjoy their favorite content at affordable prices, and more good-paying jobs will be created and preserved. As discussed above, many of today's most popular and profitable Internet services and consumer electronics devices are tied to the availability of professionally-produced music. If the Music Community continues to lose revenue to piracy, the cultural products that keep consumers interested in going online may decrease in number and quality. Thus, legitimate service providers throughout the Internet ecosystem should be self-interested in decreasing infringement.

The Music Community commends the IPEC for encouraging industry players involved in e-commerce to work together, both within their sector and across sectoral lines, to craft and implement "best practices" that will assist in the fight against online copyright theft. As noted in RIAA's comments in response to the USPTO's Request for Comments in its Voluntary Best Practices Study, voluntary initiatives promote a growing recognition among all responsible stakeholders in the Internet ecosystem that they have an important role in promoting a legitimate online environment.⁴⁹ And, as previously discussed, several such initiatives have been implemented to date with positive results.

In addition, several foreign countries have also promoted voluntary best practices, which may provide significant guidance for possibilities within the U.S. For example, the Government of France in May 2014 published *Operational Tools to Prevent and Combat Online Infringement*,⁵⁰ which highlighted and recommended important voluntary initiatives for reducing online piracy, including (1) the signature of sector charters involving the stakeholders in advertising and on-line payment (Visa, MasterCard, PayPal); (2) creation by a public authority of a list of massively infringing sites, which would be used to inform all the technical and financial intermediaries of the sites at issue; (3) the creation of an order for prolonged removal, targeting specific counterfeit content; and (4) creating monitoring arrangements of legal decisions regarding massively infringing websites to combat the reappearance of pirated content and to make sure that legal decisions were not circumvented.

Going forward, there are challenges in two areas: first, to meaningfully and constructively implement the commitments and undertakings embodied in these important initiatives; and second, to expand this trend into other areas where clear statements of industry best practices, and inter-industry cooperation to fight online copyright theft, are sorely needed. The first dimension will require follow-up and monitoring of the agreements already reached, to

⁴⁹ Comments of RIAA, USPTO's Request for Comments in its Voluntary Best Practices Study (Aug. 19, 2013), <http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf#page=15>.

⁵⁰ *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne, Rapport à la ministre de la culture et de la communication*, May 12, 2014, English Language summary available at <http://merlin.obs.coe.int/iris/2014/6/article18.en.html>.

ensure that they produce concrete results that do, in fact, help to cut off the revenue streams now flowing to online pirates. The IPEC is well situated to conduct this follow-up; to coordinate the activities of other federal agencies that have a role to play; to report on the results, as appropriate; and to encourage the parties involved to move forward on the constructive paths on which they have embarked.

Some areas where new or more refined voluntary best practices are needed include the following:

- Registrars/Registries: The Internet Corporation for Assigned Names and Numbers (“ICANN”) must play a central role to encourage increased cooperation among copyright and trademark holders and domain name registration businesses, in order to have an impact on limiting infringement. In the current transition context, ICANN needs to demonstrate publicly its stated commitment to accountability and the rule of law. Beyond encouraging voluntary initiatives and discussions, there should be explicit statements that confirm as part of ICANN’s core mission its authority to negotiate and enforce its contracts with registrars and registries – including contractual provisions targeting abusive uses of domain names. In 2013, revision of the Registrar Accreditation Agreement (“RAA”) resulted in domain name registrars taking on important new obligations to respond to complaints that domain names they sponsor are being used for copyright or trademark infringement, or other illegal activities. But registrars are not properly responding, and to date ICANN is not taking action to clarify and enforce these RAA provisions. We anticipate the same may be true in connection with rogue sites on new gTLDs. In addition, the 2013 RAA also set in motion long-overdue steps toward developing standards for the widespread phenomenon of proxy registration services. Further progress will be critical if the role of the Whois database in advancing online accountability and transparency is to be saved.

The Music Community urges the Office of the IPEC to stay actively involved in convincing ICANN, registries, registrars and privacy/proxy services that protecting copyrights and trademarks is in the best interest of the entire Internet ecosystem.

- Hosting and CDN Companies: Companies that provide such services should come to the table to discuss ways to continue delivering quality products while also respecting the property of others. We need greater certainty in the responses in the face of notices of widespread infringement, and additional efforts to ensure that a takedown notice is effective. We also need to develop a common sense approach to implementing a repeat infringer policy.
- App Stores: Far more could be done by the providers of digital storefronts where consumers locate and obtain/purchase applications for mobile devices, browser plug-ins, or software applications. Given that real world stores have to avoid distributing infringing content, there is no reason why digital storefronts cannot do more as well. While we appreciate that notice programs have been developed to address infringing apps that are available on some mobile app storefronts, we need to address how to increase the diligence so that infringing apps are more likely to be rejected before making it into the

storefront in the first place, and better tools to avoid repeat infringing apps, whether by the same developer under a different name, or a copycat app that provides substantially the same infringing service under a substantially similar name.

- Search Engines: Search engines continue to provide a critical link between online copyright theft sites and the audiences they seek to serve, including U.S. consumers. While demotion efforts have made a difference, without greater cooperation by the major search engines with right holders, online theft sites will continue to benefit from the substantial traffic sent to them by the search engines. These critical players in the e-commerce environment must be encouraged to work toward an agreed-upon framework for delisting from search results those sites that are clearly dedicated to, and predominantly used for, infringement. They also should refine their “suggested searches” functionality, so as not to drive innocent users to infringing versions of content. A strong and comprehensive set of best practices in the search engine area, similar to the principles adopted by a number of user-generated content services,⁵¹ could deliver enormous benefits to all Internet players whose interests are undermined by the prevalence of online theft, and could reduce pressure for legislative or regulatory initiatives that seek the same goal.
- Making the Standard Technical Measures Condition to the DMCA Meaningful: Reasonably priced, commercially available technologies exist today to identify and protect copyrighted works. While some service providers have implemented such measures, many others feel no compulsion to do so. The IPEC should call together service providers and copyright owners to discuss these technologies and develop “standard technical measures” around them as contemplated in 17 USC § 512(i).

B. Legislative Recommendations

The Music Community urges the IPEC to consider supporting several legislative reforms of the Copyright Act and laws impacting enforcement of the copyright laws. The areas that require the most immediate attention include: (i) the “notice and takedown” provisions of 17 U.S.C. § 512; and (ii) resolving issues related to websites located outside of the U.S.

1. Fix the DMCA

The Music Community recommends that the IPEC support revision of the notice and takedown system to update it to address the current technological environment.

- (a) Clarify that Inducers and Willfully Blind Operators have Red Flag Knowledge

The statute strips service providers who have “red flag” knowledge of infringement on their websites of safe harbor protection unless they take action to prevent or limit the

⁵¹ See Principles for User Generated Content Services, <http://www.ugcprinciples.com/>, last visited Oct. 12, 2015.

infringement. 17 U.S.C. § 512(c)(1)(A)(ii); Report of the Senate Committee on the Judiciary on S. 2037, the Digital Millennium Copyright Act, S. Rep. No. 105-190 (1998) (the “intended objective” of the “red flag” knowledge standard was “to exclude sophisticated ‘pirate’ directories—which refer Internet users to other selected Internet sites where pirate software, books, movies, and music can be downloaded or transmitted—from the safe harbor”). The statute also allows copyright owners who learn of the presence of infringing material on a website to notify the service provider of a “representative list” of infringed works and thereby cause the service provider to remove other clearly infringing material. 17 U.S.C. § 512(c)(3)(A)(ii). However, current case law has been read to allow service providers to willfully blind themselves to infringing activity while intentionally raking in profits attributable to it. Thus, many service providers refuse to respond to representative lists and ignore all infringing content until they receive particularized notices of each individual infringement from copyright owners. Even after receipt of such notices, they refuse to be proactive in any way – instead, they only remove one link to an infringed work while others remain, and allow new links to the exact same content to be added minutes later. Some social media sites invoke the safe harbors while enabling their users to shield their content from public searching – further impeding the enforcement of copyright rights. This is simply not a system that Congress ever would have designed.

Given that the statute was intended to encourage “innocent” Internet service providers to prevent or limit infringement that may arise unintentionally from their normal activities,⁵² the liability limitations should be expressly unavailable to any service provider who intentionally induces or encourages infringement, or is willfully blind to it – even if they are not aware of specific individual instances of infringement through notices from rights holders. It should clarify that red flag knowledge does not require notices of particular infringing URLs when other indicators of that infringement are apparent. Moreover, the statute should define the term “representative list,” and clarify that copyright owners can put service providers on notice of widespread and actionable infringement on their sites, thereby shifting the burden to the service providers to properly safeguard their properties.

(b) Address Repeat Infringements, Not Just Repeat Infringers

The DMCA conditions the liability limitations on the adoption and reasonable implementation of a policy to terminate the access of “repeat infringers” in “appropriate circumstances.” 17 U.S.C. § 512(i)(1)(A). However, as important as addressing repeat infringers is to address *repeat infringement*. Copyright owners should not be required to engage in the constant game of sending repeat takedown notices for the same song (or other work), simply because it appears at a marginally different URL than the first time. The current standard of “URL by URL” takedown doesn’t make sense in a world where there is an infinite supply of URLs. Technologies exist to identify content that is reposted after it is removed and they should be deployed as a standard industry practice.

⁵² *ALS Scan, Inc. v. RemarQ Communities, Inc.* 239 F. 3d 619 (4th Cir. 2001).

2. Consider an Alternative or Additional “Duty of Care” Standard

As implemented, many believe that currently, the DMCA places the burden exclusively on creators alone to police for infringing activity. Given the marketplace changes that have taken place since the DMCA was enacted, reasonable reform should attempt to balance the burden so that services seeking safe harbor protection have a heightened duty of care to establish reasonable measures to prevent infringing activity from appearing on their sites *ex ante* when it is reasonably foreseeable that such infringing activity would occur or is occurring. This could work as an alternative scheme to the DMCA or in conjunction with an improved notice and takedown (and stay down) system. Prominent scholars have advocated this recalibrated approach, which represents a return to more traditional tort principles.⁵³

3. Legislative Reform to Address Ex-U.S. Sites

The difficulty and complexity of pursuing services and sites dedicated to online theft increases when those services are hosted outside the U.S., operated by individuals or entities located outside the U.S., and/or when they rely upon domain names registered in ccTLD registries overseas or new gTLDs operated outside of the U.S. These problems can be expected to intensify. As noted above, online copyright thieves have become increasingly peripatetic and can shift their bases with increasing velocity. They are adept at jumping across borders and assuming alternate identities to evade the long arm of the law.⁵⁴

As the Obama Administration has forthrightly stated, “online piracy is a real problem that harms the American economy, threatens jobs for significant numbers of middle class workers and hurts some of our nation’s most creative and innovative companies and entrepreneurs,” and “online piracy by foreign websites is a serious problem that requires a serious legislative response.”⁵⁵ Further concerns raised with other proposed options to address this serious problem

⁵³ See Peter S. Menell and David Nimmer, *Legal Realism in Action: Indirect Copyright Liability’s Continuing Tort Framework and Sony’s DeFacto Demise*, 55 UCLA L. Rev. 1 (2007).

⁵⁴ The Pirate Bay remains a classic example. Its operators initially set it up in Sweden. After criminal and civil decisions against the operators, the Pirate Bay began changing ISPs and temporarily moved its services to the Netherlands and Germany before returning to Sweden. The Pirate Bay also registered the domain names depiraatbaai.be and baiedespirates.be, allowing Belgian users to access the site again, without using alternative DNS providers. Moreover, The Pirate Bay now has dozens of active proxies, mirrors, and clones, *e.g.*, thepiratebay.tn; thepiratebay.lv; mythepiratebay.org. See *All Pirate Bay Mirrors*, Tech Toy (Jan. 16, 2014), <http://techttoy.co.uk/pirate-bay-mirrors/>. This multiplies the number of takedown notices required to remove a single work that previously would have been hosted at only one URL.

⁵⁵ Victoria Espinel, Aneesh Chopra, and Howard Schmidt, *Combatting Online Piracy While Protecting an Open and Innovative Internet*, Jan. 14, 2012, <http://www.whitehouse.gov/blog/2012/01/14/obama-administration-responds-we-people-petitions-sopa-and-online-piracy>.

have proved to be unfounded.⁵⁶ Any updated IPEC strategy should include a review of the approaches taken by other countries to address this issue in considering how best to address this evolving problem.

C. Enforcement Recommendations

The Music Community commends federal law enforcement agencies for their vigorous and persistent efforts to use available legal tools to crack down on online copyright theft, including their recent enforcement activities in connection with the criminally infringing sites RockDizFile and ShareBeast.

However, more funding is required to sustain and enhance such efforts. Further, brazen copyright infringement must remain an enforcement priority. The economic harm, loss of livelihoods, and damage to our creative culture from these activities must not be underappreciated. We urge federal law enforcement agencies to redouble their efforts towards cracking down on online infringement, and increase cooperation with their overseas law enforcement counterparts in other countries. The increasingly trans-national character of the organized enterprises that dominate the world of online copyright theft requires this.

D. Regulatory Guidance

The Music Community urges the IPEC to consider incorporating the Copyright Office's views on the problems with the DMCA and, as applicable, requesting further guidance from the Copyright Office on the proper statutory construction of the DMCA.⁵⁷

The IPEC should also consider requesting the Federal Trade Commission to investigate and issue a report on the evolving relationship between sites/services that engage in infringement, those that support or profit from such sites/services, and cybersecurity threats posed by such sites/services.⁵⁸

IV. Conclusion

Pirates do not make copyrighted music available for free online as a public service. They make money from it: lots of money relative to the level of effort involved to engage in this behavior. They sell advertising on their services, and rake in huge profits from their illicit activity. Yet, it causes exponentially more harm to the Music Community. Unlike legitimate companies, these services have no interest in actually removing infringing files or links; their

⁵⁶ See Daniel Castro, *Oops. DNS Blocking Did Not Break the Internet* (October 12, 2015) <http://thehill.com/blogs/pundits-blog/technology/256635-oops-dns-blocking-did-not-break-the-internet>.

⁵⁷ See, e.g., *The Register's View on Copyright Review: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 1 (2015) (statement of Maria A. Pallante, Register of Copyrights and Dir., U.S. Copyright Office), http://judiciary.house.gov/_cache/files/9855f607-e28b-4ff9-b2f6-7a1106d4ce48/114-22-94408.pdf.

⁵⁸ See *supra* n. 42 for literature noting the ties between sites that engage in infringing activity and the creation of other cybersecurity risks, including malware and identity theft.

incentive is exactly the opposite – to ensure that users can access as much illegal content as possible, so that advertising revenues can continue to flow.

The important takeaway is that these services are not responsible entities who, when given notice of infringement, actually try to do something about it. These pirate services have an economic interest in ensuring that access to pirate copies remains uninterrupted, and they use technology to make that happen, regardless of how many takedown notices they get. The underlying assumption of the DMCA takedown process – that responsible entities will do the right thing and remove or disable infringing files and will not control or profit from the infringing activity – is simply not accurate with respect to these pirate operators. And the cost, complexity, broken legal framework, and resources involved with civil or criminal litigation against such operators limit the utility of those tools.

Thus, we must also look to those service providers who do represent the responsible parties envisioned by the DMCA and who provide visibility and viability to these bad online actors. And changes in the law are required to further incentivize these companies to fully engage in fighting online theft, and to discourage rogue entities from attempting to use our antiquated laws as a sword to continue their illegal activities. Although much is being done, it is far too little and is often done far too slowly. Because the success of creative industries, like the Music Community, is vital to making the Internet marketplace as successful as possible and ensuring that the rising digital tide actually lifts all boats, we ask the IPEC to consider the proposals made herein for legislative and regulatory action as well as for instigation of private cooperative efforts.

APPENDIX A

DESCRIPTIONS OF MUSIC COMMUNITY ORGANIZATIONS

American Federation of Musicians

American Federation of Musicians (AFM) is the largest organization in the world representing the interests of professional musicians. Whether negotiating fair agreements, protecting ownership of recorded music, securing benefits such as health care and pension, or lobbying our legislators, the AFM is committed to raising industry standards and placing the professional musician in the foreground of the cultural landscape.

Americana Music Association

The Americana Music Association is a professional non-profit trade organization whose mission is to advocate for the authentic voice of American Roots Music around the world. The Association curates events throughout the year including the annual Americana Music Festival and Conference in Nashville, the acclaimed Americana Honors & Awards program (and PBS special) and “Americana NYC” in partnership with Lincoln Center, New York City.

Church Music Publishers Association

The Church Music Publishers Association (CMPA), Nashville, TN, is an organization of North American and international publishers of Christian and other religious music that promotes worldwide copyright information, education, and protection. Founded in 1926, CMPA represents 56 member publishers.

Gospel Music Association

Founded in 1964, the Gospel Music Association’s purpose is to foster interest among the general public in gospel and Christian music, to build community and cooperation among industry leadership in order to address mutual business issues to maximize sales of Christian music and to promote public awareness of Christian music in our culture.

Music Managers Forum – United States

The Music Managers Forum (MMF-UF) provides a platform to connect, enhance, and reinforce the expertise and professionalism of music managers. Our goal is to further the interests of managers and their artists in all fields of the music industry, including live performance, recording and music publishing matters.

While many up and coming managers cannot easily have their voices heard or their views recognized, the MMF-US has a vital role to play in ensuring that the industry evolves fairly and profitably for all who work in the management industry and their clients. It is the goal of the MMF-US to make sure managers voices are heard. As the industry continues to evolve, the MMF-US endeavors to help its members to stay ahead of the curve.

National Music Publishers' Association

Founded in 1917, the National Music Publishers' Association (NMPA) is the largest music publishing trade association in the United States and the voice of music publishers and their songwriter partners. Its mission is to protect, promote, and advance the interests of music's creators on the legislative, judicial, and regulatory fronts.

Nashville Songwriters Association International

The Nashville Songwriters Association International (NSAI) is the world's largest not-for-profit songwriters trade association. Established in 1967, the membership of more than 5,000 active and professional members spans the United States and seven other countries. NSAI is dedicated to protecting the rights of and serving aspiring and professional songwriters in all genres of music.

Performing Rights Organizations (BMI, ASCAP, and SESAC)

BMI, ASCAP, and SESAC are the three U.S. music performing rights licensing organizations ("PROs") that collectively represent hundreds of thousands of songwriter, composer, and publisher members and combined repertoires consisting of millions of copyrighted musical works. The PROs each license the non-dramatic public performance rights in musical works to their respective repertoires on a non-exclusive basis to a wide range of users, including diverse digital broadcasting entities such as radio, television, cable, satellite and Internet services. BMI and ASCAP operate as not-for-profit businesses and return all license fees collected, less operating expenses, as royalties to their respective affiliated members whose works are publicly performed. The vast majority of BMI, ASCAP, and SESAC member songwriters and music publishers are small business men and women who depend on the PROs for collecting performing right royalties on their behalf, which constitute a major portion of their income.

Recording Industry Association of America

The Recording Industry Association of America (RIAA) is the trade organization that supports and promotes the creative and financial vitality of the major music companies. Its members are the music labels that comprise the most vibrant record industry in the world. RIAA members create, manufacture and/or distribute approximately 85% of all legitimate recorded music produced and sold in the United States.

Rhythm & Blues Foundation

The Rhythm & Blues Foundation is the pre-eminent non-profit organization dedicated to the historical and cultural preservation of Rhythm & Blues music. It provides financial and medical assistance, educational outreach, performance opportunities and archival activities to Rhythm & Blues artists and their fans.

Screen Actors Guild – American Federation of Television and Radio Artists

Screen Actors Guild – American Federation of Television and Radio Artists (SAG-AFTRA) represents approximately 160,000 actors, announcers, broadcast journalists, dancers, DJs, news writers, news editors, program hosts, puppeteers, recording artists, singers, stunt performers, voiceover artists and other media professionals. SAG-AFTRA members are the faces and voices that entertain and inform America and the world. With national offices in Los Angeles and New York, and local offices nationwide, SAG-AFTRA members work together to secure the strongest protections for media artists into the 21st century and beyond.

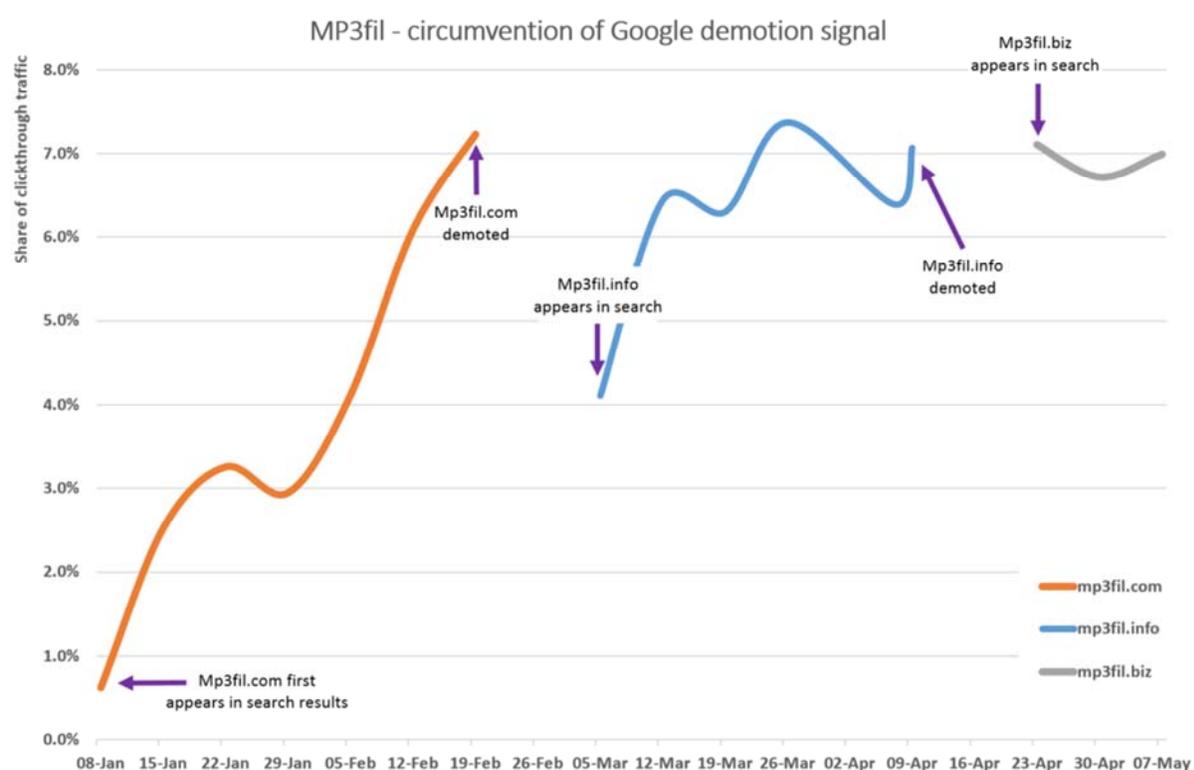
The Recording Academy

Established in 1957, The Recording Academy is an organization of musicians, songwriters, producers, engineers and recording professionals that is dedicated to improving the cultural condition and quality of life for music and its makers. Internationally known for the GRAMMY Awards® — the preeminent peer-recognized award for musical excellence and the most credible brand in music — The Recording Academy is responsible for groundbreaking professional development, cultural enrichment, advocacy, education and human services programs. The Academy continues to focus on its mission of recognizing musical excellence, advocating for the well-being of music makers and ensuring music remains an indelible part of our culture.

APPENDIX B

Apparent Impact of Domain Hopping on Search Results

The chart below shows the progress in search results of the infringing site MP3fil. This site first featured in searches for music content in January 2015 on the domain **mp3fil.com**. Over time, search results featured the site on more occasions and by 19th February 2015, the domain was listed on the first page of search results for 100 common music queries and as the first result for 12 queries. Using data that calculates typical clickthrough rates produced an estimate that 4.8% of traffic from Google searches for music content led to the Mp3fil.com domain.



During the weeks that this domain had been featured in search, the music industry had sent over 120,000 delist requests to Google for the mp3fil.com domain and a few days after 19th February, the mp3fil.com domain was demoted. However, by 5th March the site had moved to the domain **mp3fil.info** – showing exactly the same appearance and structure and with the mp3fil.com domain redirecting to the new domain. By 26th March, this domain was listed on the first page of search results for 52 out of 100 music related search queries and as the first result for 10 queries. A few weeks later, after 115,000 delist requests had been received by Google for the domain, the site was again demoted. Yet the pattern repeated once more, with the site

reappearing in search results two weeks later on 26th April on the domain **mp3fil.biz**, with the same look and feel and with both previous domains redirecting to the new destination.⁵⁹

⁵⁹ The same circumvention behavior has been observed in other sites as well. Source: Analysis by IFPI.

Appendix D

Reports Referenced in Question 29

Bruce Boyden, *The Failure of the DMCA Notice and Takedown System: A Twentieth Century Solution to a Twenty-First Century Problem*, CENTER FOR THE PROTECTION OF INTELLECTUAL PROPERTY GEORGE MASON UNIVERSITY SCHOOL OF LAW (Dec. 2013).

Liron Sivan, Michael D. Smith, Rahul Telang, *Do Search Engines Influence Media Piracy? Evidence from a Randomized Field Study*, HEINZ COLLEGE RESEARCH (Feb. 2014).

Stan J. Liebowitz, *How much of the decline in sound recording sales is due to file-sharing?*, JOURNAL OF CULTURAL ECONOMICS (Sept. 28, 2014).

“Copyright Enforcement in the Digital Age: Empirical Economic Evidence and Conclusions”, WORLD INTELLECTUAL PROPERTY ORGANIZATION ADVISORY COMMITTEE ON ENFORCEMENT, TENTH SESSION, Geneva, Nov. 23 to 25, 2015.

Appendix E
ESL Music Letter

March 28, 2016

Maria Pallante
Register of Copyright
Copyright Office
101 Independence Ave. S.E.
Washington, D.C. 20559-6000

Re: Copyright Office Study of Sec. 512 (DMCA)

Dear Register Pallante:

We are the founders and owners of the band Thievery Corporation, and the record label and music publisher ESL Music. We founded Thievery Corporation, a group specializing in a unique brand of eclectic electronic music over 20 years ago in Washington, D.C. In addition to releasing Thievery Corporation product, we also signed well over a dozen artists to our label ESL Music.

While we distributed physical product, we also sold and streamed Thievery and ESL Artist releases online, and licensed our music for worldwide advertising campaigns and for use in movies and television shows. We also achieved a good level of success touring, having performed in some of the most prestigious venues in the world, including The Hollywood Bowl, Red Rocks, and the 9:30 Club.

Unlike other artists and labels, much of our success was due to focusing on Internet distribution and promotion, working closely with our Internet aggregator/distributor INgrooves. And we did this without major radio airplay. Instead, the Internet was our primary delivery and promotional platform of choice. And we not only used the Internet to distribute our music, we used it as a means of communicating with our incredibly strong and faithful fan base.

About 12 or so years ago we started to recognize that sales were decreasing and piracy was on the rise, even as our fan base continued to increase. We knew about the increase in piracy because at times our fans actually notified us about websites offering our music for free or selling our music for almost nothing. Our fans thought this was awful and so did we. We then learned about a law that provided us with a means to stop the unauthorized use of our music. It was called the Digital Millennium Copyright Act. Essentially, all we had to do was to send “takedown notices” and the offending parties would stop. Or at least that was the promise. What actually happened was totally different.

We worked with our attorney to learn how to send takedown notices and we used our own employees to send the notices. We knew where to send many of the takedown notices because our employees were technologically savvy.

We had high hopes of stopping this unconscionable theft of our music and the music of ESL artists. But instead of stopping the piracy and unauthorized use of our music, we were met with

a different reality. Most of the takedown notices were ignored. And if our music was taken down, it would almost immediately return on another site or even the same site. We were spending more and more resources on the takedown notices, and we were consistently getting less and less in return. Eventually, we decided to stop sending the notices altogether. It was simply an exercise of throwing good money after bad.

So time and again, we released product realizing more and more that we had no real way to stop its unauthorized use and the erosion of its commercial viability. One day we recognized an awful truth. We had no real legal remedy to stop the theft of our property - period. When we release music, our control is gone. Any sales and use of our music is essentially an act of charity. If our fans or some companies want to pay, they will. But if they don't want to pay, they don't. And there is nothing we can do about it.

And for those companies wanting to pay, we now realize they will pay less and less, rationalizing the payment of low royalties by claiming getting paid micro-pennies is better than not getting paid at all. We have been told that the DMCA was supposed to place some responsibility on behalf of these companies to help address piracy, and yet we find out that the Courts have essentially interpreted the DMCA in a way that places no responsibility on those services like Google to proactively enforce our rights. With these types of laws, why would they pay us anything but micro-pennies, if that?

Even more infuriating, we were told that the ISPs had filtering technology that could be used to identify those using our music without authority. But because they are conditioned to ignore the existence of the problem, and the Courts placed no responsibility on them to pro-actively engage in anti-piracy efforts, they refused to use the technology unless you signed a deal with them. Without a strong legal deterrent mandating the use of filtering, the ISPs have no incentive to change the status quo.

Quite simply, the DMCA has failed us. And not only can we not protect our music, we cannot protect the fantastic music of other ESL artists like Federico Aubele, Natalia Clavier, Thunderball, and Nickodemus. Essentially, when we signed those artists we became the caretakers of their copyrights. And now we realize we do not have the tools to do that anymore. Partly because of this, we are releasing our artists from our label. While there are other economic and business reasons for this decision, a major one is the failure of the DMCA to provide us with a means to protect their property and to pay them what they deserve for the use of their music. Thievery Corporation will continue – and we hope to thrive – but ESL Music for other artists is no more.

We understand the Copyright Office has started a study of the DMCA and we believe it is very important for your office to understand our experience. It is gut wrenching to us that the DMCA does not provide in fact, what it promised, and you need to help Congress reform the law so that other songwriters, artists and indie labels coming after us have the proper tools to protect their music.

What most people don't understand is that this is not only a legal problem – it is a cultural catastrophe. Without properly protecting the rights of songwriters and artists, we will have less quality art and fewer quality artists. The Internet, using technology we love, should be the friend of the artist, not its enemy. The Internet is not going anywhere, but the DMCA can be changed for the better. If it is not, the Internet will not be the fantastic distribution system that everyone wants it to be. It will be nothing less than a digital tip jar. If you want to pay you can – but if you don't want to, you don't have to. What kind of copyright law allows that? The DMCA must be reformed.

Sincerely,

Eric Hilton and Rob Garza
ESL MUSIC, INC.