



**Association of American Publishers¹
Statement Submitted for the Hearing Record
House Judiciary Committee
Subcommittee on Courts, Intellectual Property, and the Internet
March 28, 2014**

**Hearing on “Section 512 of Title 17”
March 13, 2014**

Introduction

On behalf of its members, the Association of American Publishers (“AAP”) appreciates this opportunity to place its views in the hearing record of the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet (“IP Subcommittee”) regarding the current ineffectiveness² of the “notice-and-takedown system” which, in conjunction with a carefully-crafted set of liability “safe harbors,” was established in Section 512 of the Digital Millennium Copyright Act (“DMCA”) more than fifteen years ago in Congress’s initial creative and hopeful attempt to address the problem of online copyright infringement by incentivizing a collaborative response from copyright owners and Internet service providers (“ISPs”).

In particular, AAP submits this post-hearing statement to support and elaborate upon the oral and written testimony presented at the IP Subcommittee’s March 13 hearing by Paul Doda, Global Litigation Counsel for Elsevier Inc., regarding the specific nature of the problems that

¹ The Association of American Publishers (AAP) represents over 400 publishers, ranging from major commercial book and journal publishers to small non-profit, university, and scholarly presses.

² AAP intends to confine this statement to the issue discussed at the IP Subcommittee’s Section 512 hearing. Please note, however, that AAP has provided detailed suggestions for how to improve the efficiency and effectiveness of the daily operation of the notice-and-takedown process within the current terms of Section 512 as part of an ongoing inquiry by the Department of Commerce in follow up to its release of its Green Paper in 2013. *See* Department of Commerce, Request for Comment on Green Paper, Copyright Policy, Creativity, and Innovation in the Internet Economy, 78 Fed. Reg. 61,337 (Oct. 3, 2013) <http://www.gpo.gov/fdsys/pkg/FR-2013-10-03/pdf/2013-24309.pdf> (Comments of the Association of American Publishers, *submitted* (Nov. 13, 2013)).

have made the integrated system of the notice-and-takedown process and eligibility for “safe harbor” protection against copyright infringement liability incapable of achieving its intended purpose, and some concrete suggestions for how to improve the workings of that system in a continually-evolving online environment.

In noting our specific concerns and our recommendations for addressing them, AAP recognizes that voluntary “best practices” and agreements among the key stakeholders in the online ecosystem are likely to be the most practical, effective and achievable ways to improve the daily operation of the notice-and-takedown system insofar as such measures can adapt to the rapid pace of technological and entrepreneurial change on the Internet more adroitly than can federal legislative, judicial and regulatory processes. However, this submission will also touch upon Section 512-related enforcement problems which, based upon current legal, market and technological realities, will likely require federal government intervention to make these crucial elements of the overall U.S. copyright enforcement system truly *effective* in the modern online environment.

Current Ineffectiveness of Notice-and-Takedown

As was noted by several members of the IP Subcommittee and each of the hearing witnesses, successful partnerships between copyright owners and technology platforms have led today’s consumers to expect and often achieve instant online access to high-quality, copyrighted content anytime and anywhere.

All types of publishers represented within AAP’s membership -- across the trade, academic, and scientific, professional and technical sectors -- are investing and innovating to meet this demand through the production, distribution and making available of eBooks, online journals, audio-books, integrated digital learning solutions, and other new forms of works, along with new business models that take advantage of the ubiquity of the Internet to serve local, national and global markets.³

But with increasing digital adoptions and adaptations by publishers, online piracy of their works likewise continues apace, and the costly and frustrating notice-and-takedown experiences of Elsevier, as detailed by Mr. Doda in his hearing testimony,⁴ have become all too common among AAP member publishers of all types, whether large or small, for-profit or non-profit,

³ See *The Rise of Innovative Business Models: Content Delivery Methods in the Digital Age: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2013) (Post-hearing Statement of the Association of American Publishers available at <http://www.publishers.org/attachments/docs/publicstatements/aapstatement-riseofinnovativebusinessmodels.pdf>.

⁴ *Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2014) (Testimony of Paul F. Doda providing a number of illustrative examples of this “whack-a-mole” problem at 2-4).

established or start-up. Despite sending millions of takedown notices annually⁵ to remove infringing copies, or links to such copies, of their published works, AAP member publishers find themselves competing against a plethora of different sites on the Internet that persist in offering or enabling individuals to find and download illegitimate copies of virtually any popular copyrighted work they want at any time because, as the IP Subcommittee heard at the hearing, the notice-and-takedown process has become an efficient but highly *ineffective* “whack-a-mole”⁶ game.⁷

One challenge copyright owners face is that many kinds of websites and services that were never anticipated during the original legislative negotiation and crafting of the key elements of Section 512 now enjoy the DMCA’s “safe harbor” protections from infringement liability, despite having significantly different postures toward the uploading of infringing copies of copyrighted works to their systems than was evident with the original “service providers” for whom these protections were intended and designed. Although these new websites and services fall within the broad terms of Section 512’s second and far broader definition of “service provider,”⁸ they have developed lucrative new business models that are structured with features and operational behavior that attract unauthorized user uploads of copyrighted works⁹ in order to

⁵ See *Transparency Report*, GOOGLE <http://www.google.com/transparencyreport/removals/copyright/> (last visited Mar. 28, 2014) (showing that Google alone receives approximately 30 million DMCA notices per month).

⁶ The “whack-a-mole” problem describes the situation where links to infringements of copyrighted works are taken down subject to a valid takedown request only to reappear, sometimes through the exact same URL, shortly thereafter, requiring an endless cycle of takedown requests to provide even the slightest amount of protection for creative works.

⁷ While AAP commends Google for simplifying the notice sending process on its sites, creating a “trusted submitter” program for handling high volumes of automated notices from frequent submitters, and for processing notices in an average of less than 6 hours, the fact that in 2013 Google received “takedown notices for more items *every week* than [it] received in all of 2010” indicates that while sending and processing notices may have become quite *efficient* with respect to the de-listing of links by Google, the current implementation of the notice-and-takedown process is not an *effective* tool to reduce copyright infringement online.

⁸ See 17 U.S.C. §512(k)(1)(B) (broadly defining “service provider” as “a provider of online services or network access, or the operator of facilities therefor.” This definition also “includes an entity described in subparagraph (A),” which is a reference to service providers that engage in “transitory digital network communications.”) See *Capitol Records, LLC v. Vimeo, LLC*, No. 09 Civ. 10101(RA), slip op. at 12 (S.D.N.Y. Sept. 18, 2013) (explaining that “[t]his definition ‘is clearly meant to cover more than mere electronic storage lockers.’ Rather, it is ‘intended to encompass a broad set of Internet entities.’ Indeed, one court commented that the DMCA defines ‘service provider . . . so broadly that [it had] trouble imagining the existence of an online service that *would not* fall under the definitions.’”) (internal citation omitted, emphasis in the original).

⁹ Features and operational behaviors that attract unauthorized user uploads can include: providing users access to automated tools to monitor whether the content the user uploaded has been removed or disabled; without verifying permission to distribute the uploaded content, providing technologies that proliferate publicly-accessible links to content across multiple link sites; and providing payments or rewards for uploading content or links to content that is popular (likely commercially produced copyrighted material). To be clear, these are illustrative examples of the types of features and behaviors that AAP member publishers often encounter with regard to sites that persistently infringe their copyrights. However, AAP and its members recognize that there are legitimate contexts in which these features and behaviors can be found as well, such as YouTube, which helps users monetize their original content and OneLoad.com which allows *registered* users (that agree that they “will not upload any . . . copyrighted third-party content”) to “easily deploy and track videos across top video sharing, social networking and custom sites in a single step.” OneLoad, http://www.oneload.com/about/what_is (last visited Mar. 28, 2014).

drive traffic to their sites and profit from selling advertising, subscriptions, and service enhancements such as increased downloading speeds. Unfortunately, they are able to qualify for safe harbor protection and flourish to the detriment of rights holders by merely paying lip service to the other side of the DMCA's Section 512 equation, which is the protection of the rights of copyright owners. They may "expeditiously" takedown an infringing work in response to a notice from the copyright owner, while nominally implementing a "repeat infringer" policy, in order to maintain their eligibility for "safe harbor" protection against liability for such infringements; however, they do little else to prevent the same infringement, let alone others, from recurring on their sites or systems.

Under the current operation of the notice-and-takedown system, infringements thus remain too widespread, too frequent, and too persistent for any copyright owner, large or small, to locate all or even a substantial portion of such occurrences and achieve their effective removal without recurrence.

Recommendations for Effective Implementation of Section 512 Notice-and-Takedown

Develop and Implement Voluntary Standard Technical Measures

AAP agrees with the bipartisan view expressed by IP Subcommittee members Reps. Judy Chu (D-CA) and Tom Marino (R-PA) that, with respect to notice-and-takedown, "[d]oing the bare minimum is not how the law was intended to function" and "[t]akedown' should mean 'staydown.'"¹⁰ While a notice-and-takedown regime will continue to be useful, particularly for legitimate service providers with business models that are not structured or connected with behavior that attracts unauthorized uploads of copyrighted works, it cannot succeed in isolation to address the widespread infringement problem that the copyright community faces, especially if it requires repetitive notices from copyright owners and provides little incentive for service providers to prevent the re-uploading of the same infringing works that they have previously removed pursuant to prior notices from the same copyright owners.¹¹ In order to effectively address the massive and persistent infringement occurring online, service providers need to work with copyright holders to develop and accommodate the implementation of commercially reasonable and effective "standard technical measures" that do not impede the legitimate functionality of the service provider and can, at a minimum, be deployed to prevent the recurrent uploading of infringing copies of works that have been removed by the service provider pursuant to prior notices from the copyright owner.

¹⁰Rep. Judy Chu and Rep. Tom Marino, *Victims of IP Theft Need Better Protection*, THE HILL (Mar. 12, 2014) <http://thehill.com/opinion/op-ed/200630-victims-of-ip-theft-need-better-protection#ixzz2wL3650hz>.

¹¹ See *supra* note 4.

Of course, it is often loudly proclaimed that the DMCA was never intended to impose any *obligation* on service providers to help copyright owners fight online piracy of copyrighted works. Usually this assertion is based on two observations about the conditions of eligibility for safe harbor protection under Section 512: first, that taking action to remove or block access to infringing copies of copyrighted works on their sites or systems, in response to a notice from a copyright owner, is an entirely *voluntary* decision on the part of service providers, which they make depending upon whether they wish to be eligible for safe harbor protection from potential liability in connection with the posting of such copies; and, second, that Section 512(m) makes clear that nothing in Section 512 conditions safe harbor eligibility on a service provider “monitoring” its site, system or service for infringing materials or activities, or “affirmatively seeking facts indicating” the presence of such materials or activities. But the actual provisions of Section 512 and their legislative history evince a different intent of Congress.

While it is true that removing or blocking access to infringing materials or activity in response to a notice from a copyright owner *is* a voluntary decision made by the service provider in order to be eligible for safe harbor protection, the other conditions of eligibility for safe harbor protection are unquestionably mandatory. These include the requirement that a service provider “has adopted and reasonably implemented” a policy for termination (“in appropriate circumstances”) of subscribers and account holders of the service provider’s system or network who are “repeat infringers,”¹² and the requirement that a service provider “accommodates and does not interfere with standard technical measures” that are defined in the statute and used by copyright owners to identify or protect copyrighted works.¹³

The definition of “standard technical measures” qualified only those measures that “(A) have been developed pursuant to a broad consensus of copyright owners and services providers in an open, fair, voluntary, multi-industry standards process; (B) are available to any person on reasonable and nondiscriminatory terms; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.”¹⁴ Unfortunately, while a report of the House Judiciary Committee confirmed in its analysis of this provision that Congress “expected that all of the affected parties will expeditiously commence voluntary, inter-industry discussions to agree upon and implement the best technological solutions available to these goals” of protecting copyrighted works,¹⁵ the prescribed process for bringing them into existence never occurred.

¹² See *infra* at 9-10 (discussing the repeat infringer requirements of 17 U.S.C. §512 (i)(1)(A)).

¹³ 17 U.S.C. §512 (i)(1)(B),(i)(2). A third mandatory condition of eligibility, designating an agent to receive notifications of claimed infringements from copyright owners and providing publicly accessible contact information for such agent, applies only to the safe harbor under Section 512(c) for infringement of copyright based on a service provider’s storage of information of material on its system or network at the direction of a user of such system or network. See 17 U.S.C. §512(c)(2).

¹⁴ 17 U.S.C. §512(i)(2).

¹⁵ H. Committee Print, Serial No 6, 105th Cong., 2d Sess. (September 1998) at 37.

Still, the intent of Congress that the Section 512 safe harbors from infringement liability would apply to a service provider “only if” it “accommodates and does not interfere with” such “standard technical measures” is clearly stated in that section. Moreover, despite the common insistence that Section 512(m) absolutely rejects the proposition that the applicability of the safe harbors is conditioned on a service provider “monitoring its service or affirmatively seeking facts indicating infringing activity,” such references usually fail to note the complete phrasing of that provision, which ends with the words “except to the extent consistent with a standard technical measure complying with the provisions of subsection (i).” In this context, the requirement for *accommodation*, rather than merely non-interference, is evidence that Congress intended service providers to be *obligated* to work with copyright owners to combat online piracy of copyrighted works.

Although the “standard technical measures” required to activate that obligation do not yet exist, legitimate content sites, such as YouTube and Scribd, have *voluntarily* developed and implemented technical measures to prevent the appearance (and reappearance) of infringing content on their sites. These voluntarily-implemented technical measures not only offer an effective tool to decrease the prevalence of infringement on their sites, but also improve the efficiency and effectiveness of the notice-and-takedown process by ending the “whack-a-mole” game, and in turn, substantially eliminate the need for rights holders to send repeated notices for repeated processing by the service provider. Moreover, the technical measures adopted by these legitimate sites, which vary in size and content,¹⁶ clearly establish that such measures can be tailored and implemented in ways that are both economically and technically feasible as part of a diverse array of not only sustainable, but growing, business models.¹⁷

¹⁶Scribd.com primarily hosts literary content, whereas, YouTube primarily hosts audio and visual copyrighted content.

¹⁷ YouTube’s implementation of Content ID illustrates that commercially reasonable upload filtering can complement the growth of legitimate content-driven websites. YouTube started experimenting with its Content ID system in 2007 and now uses the system to scan over 400 years of video every day. Over this same time period, YouTube has experienced exponential growth in its popularity as illustrated by the increase from receiving/processing an average of six hours of video uploads per minute in 2007, to 24 hours per minute in 2010, 72 hours per minute in 2012, and over 100 hours per minute today. *Compare, YouTube Uploads Hit 72 Hours A Minute: How Can That Ever Be Pre-Screened For ‘Objectionable’ Material?*, TECHDIRT (May 23, 2012) <https://www.techdirt.com/articles/20120521/12065919003/youtube-uploads-hit-72-hours-minute-how-can-that-ever-be-pre-screened-objectionable-material.shtml> (noting that “some governments [are calling for] Google and others [to] pre-screen user-generated material. Just how do they think anyone can do that when every second there’s one or more hours of new material flooding in? The challenge is particularly acute for video, which does not lend itself to automatic screening, unlike text, say.”); *How Google Fights Piracy*, GOOGLE 9-10 (Sept. 2013) <https://docs.google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit?pli=1> (describing Content ID as a win-win solution for YouTube and rights holders); *Statistics – YouTube*, <http://www.youtube.com/yt/press/statistics.html> (last visited Mar. 28, 2014) (giving updated statistics on how much video content is filtered by Content ID each day). Scribd.com, which implemented its upload filter in 2009 (See FAQs, *How Does Scribd Help Protect the Rights of Authors?*, SCRIBD (Feb. 26, 2009) <http://support.scribd.com/entries/25057-How-does-Scribd-help-protect-the-rights-of-authors->) has also grown its business, launching one of the first and most comprehensive eBook subscription services in late 2013, partnering with a number of AAP member publishers. See Press Release, *The New Scribd*, SCRIBD (Oct. 1, 2013) <http://blog.scribd.com/2013/10/01/the-new-scribd/>.

With technologies that provide reasonable measures to prevent the reappearance of infringing content growing increasingly effective and affordable,¹⁸ there is no reason not to work toward development of the standard technical measures that Congress factored into its crafting of the DMCA fifteen years ago.

Increasingly, rights holders and certain service providers have realized that the most effective way to protect copyrighted works, meet consumer demands, and facilitate the growth of legitimate user-generated content sites is through a partnership between copyright holders and service providers. Specifically, this partnership involves cataloguing hash identifiers for infringing files as well as investment in creating metadata and fingerprint files for each copyrighted work to include in databases that service providers can automatically compare against potential uploads to their sites. When an exact match to the fingerprint of a copyrighted work is identified, the service provider and the rights holder can implement a pre-negotiated response, *i.e.*, allow the upload and monetize the content or block the upload. As Google has said, its Content ID technology (which implements the partnership just described) is “not just an *anti-piracy solution*, but *also a new business model* for copyright owners and YouTube alike... [that] is *good for users* as well.” When service providers accommodate this new mode of online copyright protection, everybody wins.

Currently, however, there are few incentives for service providers to voluntarily implement such measures, despite the fact that Section 512(i) of the DMCA makes clear that Congress fully expected that the content and service provider industries would develop and adopt “standard technical measures” by which copyright owners would be permitted to identify and protect copyrighted works with the cooperation of service providers.¹⁹ AAP believes that the IP

¹⁸There are a number of companies offering technological measures to protect sites against unauthorized posting of copyrighted content, with a variety of pricing and implementation models. *See e.g.*, Audible Magic <http://audiblemagic.com/solutions-compliance.php> (last visited Nov. 13, 2013) (providing “turnkey compliance and filtering solutions powered by sophisticated and patented digital fingerprinting technology”); Gracenote, http://www.gracenote.com/case_studies/itunes/ (last visited Nov. 13, 2013) (being used for more than “filtering” as it underlies iTunes Match as well); Vobile, <http://vobileinc.com/> (last visited Nov. 13, 2013); Sandvine <https://www.sandvine.com/downloads/general/success-stories/success-story-40-successful-value-added-services-deployments.pdf> (last visited Nov. 13, 2013) (explaining how its service allows broadband networks to efficiently and cost-effectively filter content).

¹⁹ As noted above, 17 U.S.C. §512(i) entitled “Conditions for Eligibility,” makes clear that to be eligible for any DMCA safe harbor, a service provider must “accommodate[] and [] not interfere with ‘standard technical measures[,]’” which are “used by copyright holders to identify or protect copyrighted works and...have been *developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process.*” Furthermore, Section 512(m) was originally included in the DMCA to protect the privacy of Internet users¹⁹, and it expressly limits its “no duty to monitor” provision by referencing the standard technical measures Congress intended ISPs and content companies to develop through the multi-industry process described in 512(i). Despite this clear limitation to Section 512 (m) and Congress’ intention in enacting 512(i), work to develop and implement such standard technical measures has not materialized. In fact, as Professor O’Connor’s testimony argues, web companies today are dis-incentivized from taking steps they would otherwise voluntarily take to ensure that copyright infringements do not appear on their website. *See Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2014) (Testimony of Professor Sean M. O’Connor at 2-3). This situation has been exacerbated by

Subcommittee and Congress should encourage and provide incentives for all stakeholders to engage in a public discussion about practical and effective upload filtering tools. A multi-industry body representing the various stakeholders involved in online copyright protection should be brought together under the guidance and supervision of the National Institute of Standards and Technologies (“NIST”) (or another government agency with the requisite technological expertise) to identify or devise a wide range of generic technical measures that service providers could voluntarily implement to reduce infringement without materially impeding the legitimate functionality of their sites.²⁰

While there have been private agreements and white papers developed in the past few years on this topic, AAP is encouraged to see that a broader and more positive public discussion of automated filtering to screen out unauthorized uploads of copyrighted works that match content previously removed in response to a valid takedown notice is now starting to happen. For example, although several years old and limited to audio and visual content, the *Principles for User Generated Content Services* (“UGC Principles”) that were developed by content and service providers in 2007 demonstrate the feasibility of reaching mutually acceptable solutions for content and service providers in the online environment. The UGC Principles demonstrate a shared commitment to: (1) eliminating infringing content; (2) encouraging dissemination of “wholly original and authorized user-generated” content; (3) protecting user privacy; and (4) accommodating fair uses of copyrighted content.²¹ Additionally, the *Fair Use Principles for User Generated Video Content* (“Fair Use Principles”), endorsed by the Electronic Frontier Foundation and other public interest organizations,²² help to identify a threshold for applying automated upload filtering to clear instances of infringement.

To be clear, AAP rejects the notion that any automated system can effectuate a valid fair use analysis or that rights holders have an obligation under the DMCA or Section 107 of the

additional case law adopting a “volitional act” requirement in order to prove infringement, which has suggested that the operator of an automated infringement machine would not be held liable. *See, e.g., Cartoon Network, LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008).

²⁰ In response to the Internet Policy Task Force’s Green Paper inquiry, AAP has recommended the “creation of a multi-industry body [to be] led by the National Institute of Standards and Technology (NIST) to devise a wide range of generic technical measures that ISPs can implement to reduce infringement without materially harming the legitimate functionality of the sites. Different types of technical measures can be developed for different types of ISPs. High volume ISPs that upload and download all types of content would obviously need a different type of technical measure than a small ISP that posts modest numbers of links to content stored at other locations. The goal of the multi-industry process would be for NIST to provide ISPs with a menu of potential technical measures they can adopt depending on their size and functionality.” *See* Department of Commerce, Request for Comment on Green Paper, Copyright Policy, Creativity, and Innovation in the Internet Economy, 78 Fed. Reg. 61,337 (Oct. 3, 2013) <http://www.gpo.gov/fdsys/pkg/FR-2013-10-03/pdf/2013-24309.pdf> (Comments of the Association of American Publishers, *submitted* (Nov. 13, 2013)).

http://www.ntia.doc.gov/files/ntia/association_of_american_publishers_comments.pdf.

²¹ *Principles for User Generated Content Services*, <http://ugcprinciples.com/index.html> (last visited Mar. 28, 2014).

²² The following groups have endorsed these Principles: Electronic Frontier Foundation; Center for Social Media, School of Communications, American University; Program on Information Justice and Intellectual Property, Washington College of Law, American University; Public Knowledge; Berkman Center for Internet and Society at Harvard Law School; and ACLU of Northern California.

Copyright Act to conduct such an analysis before sending a takedown notice.²³ However, publishers believe that Section 2(a), *i.e.*, the “Three Strikes Before Blocking” test, articulated in the Fair Use Principles, is a useful starting place for discussing how to apply automated filtering to all types of copyrighted content upon upload in a reasonable manner that provides technological safeguards against blocking fair uses.²⁴

Although these existing principles each contain useful guidelines for reasonable automated upload filtering, AAP’s recommendation to create a range of appropriate standard technical measures for different types of content and service providers requires a neutral third-party with technical expertise, such as NIST, to ensure that commercially reasonable and effective technical measures are created in a manner that accommodates the needs of various stakeholders (*i.e.*, a reasonable and effective technical measure for a high volume ISP that facilitates uploads and downloads of all types of content may differ from a reasonable and effective filter for a small ISP that posts modest numbers of links to content stored at other locations).

Develop and Implement Repeat Infringer Policy Best Practices

In addition to the current lack of incentives to voluntarily implement efficient upload filtering systems to decrease the prevalence of identified infringements on content hosting sites, the general failure of service providers to adequately or consistently adopt and implement an effective “repeat infringer” policy has also contributed significantly to the persistence and reappearance of copyright infringements.

The DMCA, in section 512(i)(1)(A), conditions an ISP’s receipt of safe harbor protection on the adoption and reasonable implementation of a “repeat infringer” policy that provides for the “termination” of an ISP’s subscribers or account holders in “appropriate circumstances.”²⁵ Congress, however, did not define reasonable implementation or “appropriate circumstances,” which has enabled ISPs to adopt varying policies without providing transparency to document the regular and reasonable implementation of such policies. Transparency is critical in evaluating the efficacy of such policies. A recent case, *Disney v. Hotfile*, illustrates just how important the reasonable implementation of a “repeat infringer” policy can be to successfully rooting out a substantial portion of the copyright infringements available online.

²³ AAP members believe the district court’s contrary ruling in the *Lenz* case, now on appeal, is without precedent and clearly erroneous as a matter of law. See *Lenz v. Universal Music*, 2013 WL (N.D. Cal Jan. 24, 2013).

²⁴ See *Fair Use Principles for User Generated Video Content*, <http://www.eff.org/pages/fair-use-principles-user-generated-video-content> (last visited Mar. 28, 2014) (suggesting that, for filtering purposes, only matching copies where “nearly the entirety (e.g., 90% or more)” of the challenged content is comprised of a single copyrighted work should be presented or removed.” AAP member publishers agree with the goal of carefully ensuring that reasonable technical measures only prevent or remove clear infringements.

²⁵ 17 U.S.C. §512(i)(1)(A).

Specifically, in the *Hotfile* case, there was no dispute as to the fact that “24,790 [Hotfile] users had accumulated more than three [DMCA] notices [identifying copyrighted works that such users had uploaded without rights holder permission]; half of those had more than *ten* notices; half again had 25 notices; 1,217 had 100 notices; and 61 had more than 300 notices.”²⁶ Furthermore, the court found that, “while those who were the subject of more than three infringement notices made up *less than one percent* of all of Hotfile’s users, they were responsible for posting 50 million files...representing 44 percent of all files ever uploaded to Hotfile” and “those same files were downloaded nearly 1.5 billion times, representing roughly half of all downloads ever from Hotfile.”²⁷

These facts show that a reasonable “repeat infringer” policy that revokes user access after accumulating multiple DMCA notices is a focused measure to address “a discreet [sic] group of problematic users” that contribute a disproportionate share of online infringements.²⁸ AAP therefore urges that Congress’s original intent should be effectuated, so 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.”²⁹ Clear, transparent, and effective “repeat infringer” policies are in the best interest of legitimate service providers, consumers and rights holders. AAP believes that these stakeholders can, with the encouragement of Congress, work together to develop best practices for implementing effective “repeat infringer” policies, which would, at a minimum, include:

- a baseline for what actions characterize a user as a repeat infringer;
- criteria for appropriately tracking repeated infringing activity³⁰, including parameters for user identification tools on sites that allow users to upload and distribute content; and
- protocols for notifying copyright owners about repeat infringer activity.³¹

Also, as these policies affect users, the best practices should require each service provider to make its specific “repeat infringer” policy publicly available in simple terms on its site.

²⁶ *Disney Enterprises, Inc. v. Hotfile Corp.*, Case No. 11-20427, slip op. at 19 (S.D. Fla Sept. 20, 2013).

²⁷ *Id.* at 20-21.

²⁸ *Id.* at 20.

²⁹ H.R. Rep. No. 105-551(II) at 61 (1998) (emphasis added).

³⁰ The service provider would need to be able to establish a connection between an infringement notice; the infringing file; and the uploader of the infringing file and also to prevent terminated users from continuing to infringe with new usernames.

³¹ See Comments from AAP in response to U.S. Patent & Trademark Office, Notice of Inquiry - Voluntary Best Practices Study, 78 Fed. Reg. 37,210 (Jun. 20, 2013), submitted Aug. 21, 2013, <http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf> (suggesting information that would be useful to provide to rights holders, including: titles, actions taken by the ISP, identity of infringers).

Promote Legitimate Content through Search Engines

As noted in AAP’s statement submitted after the IP Subcommittee’s hearing on “The Role of Voluntary Agreements in the U.S. Intellectual Property System,” our members believe that “search engines are the main gateway through which a consumer, wittingly or unwittingly, is directed to the sources of infringing content online. However, search engines have yet to commit to meaningful discussions with content creators on how to better refine search protocols to avoid serving up infringing links or sites to consumers.”³²

To be sure, Google “believe[s]” that its efforts to incorporate the “number of valid copyright removal notices [it] receive[s] for any given site as a signal in [its] ranking algorithm” should “help users find legitimate, quality sources of content more easily” given that “sites with high numbers of removal notices *may* appear lower in search results.”³³ However, as Rep. Chu’s search for *12 Years A Slave* and *Frozen* during the Section 512 hearing illustrated, links to sites offering infringing content and receiving substantial numbers of takedown notices still appear in the top of Google’s search results.³⁴ The Recording Industry Association of America has similarly found that sites making available infringing music downloads, which have received millions of takedown notices, are still showing up in the top 5 search results on Google despite its current methodologies for adjusting its algorithm.³⁵ Moreover, Google Search’s autocomplete feature often helps users find infringing material by suggesting, after the user types the title of a commercial copyrighted work, the addition of search terms such as “free,” despite the fact that the user did not include that term in their search query.³⁶

³² *The Role of Voluntary Agreements in the U.S. Intellectual Property System: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2013) (Post-hearing statement of the Association of American Publishers available at http://www.publishers.org/_attachments/docs/publicstatements/aapstatement-roleofvoluntaryagreements.pdf).

³³ *How Google Fights Piracy*, GOOGLE 14, 18 (Sept. 2013) <https://docs.google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit?pli=1>.

³⁴ *See Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2014) (Statement of Rep. Judy Chu (D-CA) conducting a live search for *Twelve Years a Slave* and *Frozen* using Google Search during the hearing and noting that, in both cases, Google Search displayed sites offering to let her watch the content “online free” in the top three search results.).

³⁵ *See The Role of Voluntary Agreements in the U.S. Intellectual Property System: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2014) (Testimony of Cary Sherman stating that “on a search conducted August 29, 2013 for mp3s or downloads of the recent top 50 billboard tracks, www.mp3skull.com, a site for which Google has received over 1.25 million copyright removal notices, showed up in the top 5 search results 42 times.”); see also RIAA, “Six Months Later – A Report Card on Google’s Demotion of Pirate Sites” (Feb. 21, 2013) <http://76.74.24.142/3CF95E01-3836-E6CD-A470-1C2B89DE9723.pdf>.

³⁶ *See Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2014) (Statement of Rep. Judy Chu (D-CA) conducting a live search for *Frozen* using Google Search during the hearing and clarifying for the record that although she did not include the term “free” in her query, Google autocomplete suggested the term and Google Search displayed a site offering to let her “watch *Frozen* online free” as the top search result.).

Search engines are a critical part of daily-life and the modern online ecosystem as illustrated by the addition of the verb “google” in the *Merriam-Webster Collegiate Dictionary*,³⁷ the *Oxford English Dictionary*³⁸ and the selection of the verb “google” as the “most useful word of 2002” by the American Dialect Society³⁹ in recognition of the “popularity and dominance of the eponymous search engine.”⁴⁰ No review of Section 512 or attempt to effectively update the notice-and-takedown process would be sufficient without addressing the prevalence of links to infringing copyrighted content in search results. Therefore, AAP asks Congress to encourage search engines to meaningfully engage with copyright owners to use technology to decrease the prevalence of links to infringing content in top search results and to avoid directing users to such links through autocomplete suggestions.⁴¹

Additional Measures to Address Sites that Attract Infringement and Non-Compliant ISPs

While voluntary adoption, implementation and accommodation of “standard technical measures,” along with adherence to best practices for “repeat infringer” policies, may go a long way in diminishing the availability of files that infringe entire copies of copyrighted works, there remain two types of sites that may require additional judicial intervention in order to secure effective copyright enforcement to combat online infringements: (A) Sites with Business Models and Behaviors that Attract Infringement and (B) Non-Compliant Sites.

A: Effective Injunctive Relief against Sites with Business Models and Behaviors that Attract Infringement

Based on the publishing industry’s experience with the notice-and-takedown system, AAP’s members have found that some sites have developed business models that attract unauthorized uploading, re-uploading and public sharing of files that infringe copyrighted works. Under such business models, even where these sites comply with takedown requests and qualify for the DMCA’s safe harbor protections, the result is, at best, a temporary disruption in the continued availability of the infringing content. To address this problem, AAP urges that, with

³⁷ Glen Chivers, *Google Enters the Dictionary*, BIT-TECH (Jul. 8, 2006) http://www.bit-tech.net/news/bits/2006/07/08/google_enters_the_dictionary/1.

³⁸ Barry Schwartz, *Google Now a Verb in The Oxford English Dictionary*, SEARCH ENGINE WATCH (Jun. 29, 2006) <http://searchenginewatch.com/article/2058373/Google-Now-A-Verb-In-The-Oxford-English-Dictionary>.

³⁹ American Dialect Society, *2002 Words of the Year*, (Jan. 13, 2003) http://www.americandialect.org/2002_words_of_the_year.

⁴⁰ *Google(verb)*, WIKIPEDIA [http://en.wikipedia.org/wiki/Google_\(verb\)](http://en.wikipedia.org/wiki/Google_(verb)) (last visited Mar. 28, 2014).

⁴¹ Note that the French Supreme Court, in Cour de Cassation Arrêt n° 832 du 12 juillet 2012 (11-20.358), ruled that “a search engine that systematically sends users, by automatically suggesting key words associated with their queries, to websites containing music files made available to the public without the consent of the files’ authors should be considered as providing the means to infringe copyright and related rights.” Furthermore, the French Supreme Court held that “stopping the automatic association of key words with terms contained in the queries are justified, even if the measures are not totally effective.” Terms at issue included “torrent,” “Megaupload,” and “Rapidshare.” Library of Congress Law Library, France: Cour de Cassation Decision on Google, http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403261_text (Aug. 1, 2012).

respect to sites that exhibit such behaviors or operate under a business model that attracts unauthorized uploading, re-uploading and public sharing of copyrighted works,⁴² courts should exercise their discretion under current law to order limited injunctive relief requiring such sites to prevent the re-upload of specific works in suit even where a safe harbor against monetary damages may apply.⁴³ Service providers can comply with this limited injunctive relief by adopting commercially reasonable and effective technical measures or other measures the court may recommend to decrease re-uploads of the same works on the site.⁴⁴ The non-exclusive factors that a court should consider in determining whether a site has a business model that attracts infringement include:

- whether the service provider’s behavior increases infringement;
- whether the service provider allows users to upload anonymously;
- whether the service provider rewards or incentivizes users for uploading content that is likely infringing;
- whether the service provider enables the uploader to obtain a link to publicly distribute their uploaded content; and
- whether the service provider allows unlimited downloading by anonymous third parties unknown by the uploader;⁴⁵
- whether the service provider has failed to adopt commercially reasonable technical measures suitable to its service to reduce infringement
- whether benefits realized by the service provider can be attributed to infringement, e.g., increased traffic to their site and/or increased profit from selling advertising, subscriptions, and service enhancements such as faster downloading speeds; and

⁴² Including torrent sites that host material that supports infringing activity. *See Columbia Pictures v. Gary Fung*, 710 F. 3d 1020 (9th Cir. 2013) (holding that torrent sites technically come under 512(c) (in addition to 512(d)), because, although they do not host the actual infringing content, they host torrent files which help site users find infringing content available from third-party P2P network users. The resulting infringement constitutes an infringing “activity using the material on the system” under 512 (c), the “material” being the torrent files contained on the torrent site.).

⁴³ 17 U.S.C. §512(c) and §512(j) provide that courts can grant injunctive relief even if monetary relief is precluded by the safe harbor. 17 U.S.C. §512(c)(1) states that “[a] service provider shall not be liable for monetary relief, or, *except as provided in subsection (j)*, for injunctive or other equitable relief.” (emphasis added). 17 U.S.C. §512(j) states that “[t]he following rules *shall apply* in the case of *any* application for an *injunction* under Section 502 *against a service provider that is not subject to monetary remedies...*” (emphasis added).

⁴⁴ This suggestion stems from German case law, where a site or service that operates or is structured in a way that increases the likelihood that it will be used for infringement has an increased obligation to take measures to prevent infringement. This “proportionality test” under German law requires that the ISP take measures that are proportionate to the likelihood of infringement by or through the ISP, taking into consideration the cost and effectiveness of the measures. This test was used in a suit brought by book publishers in Germany against *Rapidshare*, and resulted in Rapidshare ultimately adopting a filter to limit infringement of books on its service. *See* Translation, Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 15, 2013, I ZR 79/12 (Ger.) (on file with author).

⁴⁵ These features are distinguishable from legitimate cloud storage services, e.g., Dropbox.com, that incorporate safeguards such as upload limits, securing accessibility of content to intended recipients, requiring users to register even to use the site’s free service, and clear reminders that users cannot upload infringing content. *See generally* <https://www.dropbox.com/> (last visited Mar. 28, 2014) (emphasizing on the homepage that Dropbox is for making “Your Stuff” available anywhere).

- the overall quantity or percentage of infringements or links (as compared to non-infringing content or links) to infringements on the site.

Ultimately, the determination as to whether the service provider has taken adequate steps to address the infringement on its site will be up to a court to decide based on a balancing test, taking into account the various needs of the service provider, its users, and copyright owners. In general, publishers believe that the substantiality of the technical measures required of a particular service provider should increase relative to how much its business model encourages infringement, the volume of infringing activity on its site, and the level of financial gain to the service due to the infringing activity. In doing so, the cost of implementing such measures would be borne by those that are more likely profiting from the presence of infringement on their site or service.

B: Non-Compliant ISPs

The most egregious ISPs, however, simply ignore notices (“Non-Compliant” ISPs), with their operators knowing that they can hide their identities to be safe from suit or base their operations in jurisdictions outside the United States where our copyright law would not hold them responsible for the infringement they foster or promote (e.g. The Pirate Bay). Despite what seems like universal condemnation of these sites, they continue to get rich by relying on users and otherwise legitimate businesses in the U.S. to support their infringement-encouraging business models. They often market their sites or services to U.S. users (visible in the U.S. through search engines like Google, Yahoo and Bing), register their sites through U.S. domain registrars, host their sites through U.S. hosting companies, contract with U.S. ad placement services, or collect monies using U.S. payment providers. These legitimate third-party services often play a pivotal, if sometimes unwitting, role in supporting such Non-Compliant ISPs.

Non-Compliant ISPs are not responsive to traditional notice-and-takedown processes, incentives to adopt technical measures, or court orders. Therefore, to effectively address the copyright infringement on such ISPs, AAP agrees with Google,⁴⁶ the Office of the Intellectual Property Enforcement Coordinator (“IPEC”),⁴⁷ and many other stakeholders that the solution is the “follow-the-money” approach, *i.e.*, remove the financial support provided to these ISPs by third-party services.⁴⁸

⁴⁶ *Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2014) (Testimony of Katherine Oyama at 8, noting that Google has “long said that the most effective way to combat rogue sites that specialize in online piracy is to attack their sources of revenue. These sites are almost exclusively for-profit enterprises, and so long as there is money to be made by their operators, other anti-piracy strategies will be far less effective.”).

⁴⁷ See generally, Office of the Intellectual Property Enforcement Coordinator, *2013 Joint Strategic Plan on Intellectual Property Enforcement*, Jun. 2013, <http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf>.

⁴⁸ See e.g., Digital Citizens Alliance, *Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business: A Report on the Profitability of Ad-Supported Content Theft* (Feb. 2014)

While AAP commends the work of IPEC, the payment processors, ad networks and many copyright industry groups to develop best practices to start voluntary arrangements to implement a “follow-the-money” approach, it may be necessary for courts to take this approach one step further. Specifically, where a U.S. court with jurisdiction over a “Non-Compliant ISP” finds that it does not qualify for protection under any safe harbor under the DMCA and that the ISP is liable for copyright infringement, the court should have authority to enter orders requiring third parties located in the U.S. that provide services to the ISP — including advertising placement services, payment processors, search engines, server hosts, and domain name registrars — to suspend those services.

Conclusion

AAP appreciates this opportunity to give the IP Subcommittee the publishing industry’s perspective on whether the current implementation of Section 512 of the DMCA is effectively balancing the diverse rights and obligations of copyright owners, service providers and users. Publishers are rapidly expanding their business models to embrace new opportunities for distributing digital content online and hope that Congress can encourage stakeholders to work together to embrace efficient, effective, and reasonable technical measures to spur continued growth of a legitimate online environment that encourages freedom of expression, provides effective copyright protection, and fosters innovation. We look forward to continued engagement with the IP Subcommittee as it undertakes future hearings on other copyright issues.

Sincerely,



Allan Adler
General Counsel
Vice President for Government Affairs
Association of American Publishers
455 Massachusetts Ave. NW
Washington, D.C. 20001

www.digitalcitizensalliance.org/followtheprofit (providing the results of a “research project [conducted by MediaLink that] analyzed advertising-supported web sites that dealt primarily in pirated content.” The results include that the sites studied accounted for “\$227 million in annual ad revenue,” that the “30 largest sites studied that are supported only by ads average[d] \$4.4 million annually,” and that “[e]ven small sites can make more than \$100,000 a year from advertising.”); see also *International Anti-Piracy Caucus of the H. Comm. on the Judiciary*, 113th Cong. (2014) (Dear Colleague Letter reporting on the Digital Citizens Alliance report described above to reiterate the Caucus’s request for ad networks “to adopt more effective controls to prevent ads from being served to sites dedicated to trafficking in stolen goods.”).