



copyright alliance

Connecting creators · Protecting creative work

**BEFORE THE  
U.S. COPYRIGHT OFFICE**

**Section 512 Study**

**Docket No. 2015-7**

**COMMENTS OF THE COPYRIGHT ALLIANCE**

**Introduction**

The Copyright Alliance appreciates the opportunity to respond to the Notice of Inquiry that seeks input on the Section 512 study.

The Copyright Alliance is the unified voice of the copyright community, representing the interests of thousands of individuals and organizations across the spectrum of copyright disciplines.<sup>1</sup> The Copyright Alliance is dedicated to advocating policies that promote and preserve the value of copyright, and to protecting the rights of creators and innovators. The individual creators and organizations that we represent rely on copyright law to protect their creativity, efforts, and investments in the creation and distribution of new copyrighted works for the public to enjoy.

The Digital Millennium Copyright Act (DMCA) was enacted at a time when the Internet

---

<sup>1</sup> The Copyright Alliance is a non-profit, public interest and educational organization that counts as its members over 15,000 individual creators and organizations across the spectrum of copyright disciplines. The Copyright Alliance represents the interests of authors, photographers, performers, artists, software developers, musicians, journalists, directors, songwriters, game designers and many other individual creators. The Copyright Alliance also represents the interests of book publishers, motion picture studios, software companies, music publishers, sound recording companies, sports leagues, broadcasters, guilds, unions, newspaper and magazine publishers, and many more organizations.

was in its infancy. In passing the notice and takedown provisions in Section 512 of the Act, Congress intended to encourage copyright owners and online service providers (OSPs) to work together to combat existing and future forms of online infringement.<sup>2</sup> This approach was designed to remedy hardships faced not only by large copyright owners and OSPs, but also individual creators who undeniably lack meaningful tools to fight online infringement. At the outset, Section 512 seemed to have achieved Congress's purpose; but court rulings and other unanticipated changes in the online environment have rendered these provisions less effective, creating an ecosystem where mass copyright infringements are an unfortunate and regular occurrence. While Section 512 remains a workable legal framework, it is evident that the statute is under strain and that additional stakeholder collaboration is needed in order for the statute to live up to its potential as imagined by Congress.

Eighteen years have now passed since the DMCA was enacted, and the interconnectivity provided by the Internet has fundamentally changed commerce, communication, and the way the public experiences copyrighted works. Consumers can access and enjoy all sorts of copyrighted works where and when they want, and creators benefit from new platforms that reach new audiences. But at the same time, online infringement is now rampant, causing widespread harm to the economic and creative vibrancy of the copyright community. Lisa Hammer is a musician and filmmaker who had to abandon her music career because of piracy, and now her film career is approaching a similar fate. She made only about \$100 off of her latest feature film, because free illegal copies of the work are so widely available on the Internet. "I used to make money through distribution on tapes and DVDs, and even a few VOD," she said.<sup>3</sup> "But now, as soon as I release a film through an online distributor, or submit it to a film festival, I see [illegal] links to the film." A most unfortunate result for a creator who spent "thousands of hours and dollars studying filmmaking, music, and acting."

Congress struck a balance with the DMCA. In exchange for taking down infringing

---

<sup>2</sup> See H.R. Rep. No. 105-796, at 72 (1998).

<sup>3</sup> Lisa Hammer, *Stand Creative Series*, CREATIVEFUTURE (Feb. 22, 2016).

content, an OSP who is not responsible for the infringement receives a safe harbor from monetary liability—but only if they comply with additional obligations, including: implementing a repeat infringer policy; registering an agent with the Copyright Office; and responding to infringements “expeditiously” once they have actual or apparent knowledge of them. Without these additional obligations, copyright owners (especially individual creators) stand little chance against advanced online infringement.

The voluntary adoption of technologies have helped address many of the logistical hurdles of locating infringements, and sending and processing hundreds of millions of takedown notices per year; however, it is essential that these technologies continue to be improved in order to keep pace with new technologies and new types of online infringement. In addition, more needs to be done to ensure that individual creators, who are the lifeblood of the creative community, are not left behind in a world where human review alone is no longer practical. Finally, the courts need to ensure that bad actor OSPs do not continue to operate under the protection of the Section 512 safe harbors. The courts should also ensure that the underlying goals of the DMCA and the intent of Congress are effectuated by, for instance, enforcing Section 512’s statutorily-required repeat infringer policies; properly applying the red flag knowledge standard; and recognizing the flexibility provided in the “representative list” language.

The copyright community stands ready to work with the Copyright Office, the Administration, and other stakeholders to ensure that Section 512 is an effective and meaningful statutory scheme to combat online infringement in the digital world. We seek to revitalize the spirit of cooperation between the copyright community and OSPs that Congress intended when it drafted and passed the DMCA. Congress recognized that cooperation would lead to the most beneficial, effective enforcement of the law. It is time for stakeholders to take voluntary action, and for the courts to effectuate Congress’s intention that copyright affords “effective—not merely symbolic—protection.”<sup>4</sup>

---

<sup>4</sup> Sony Corp. of America v. University City Studios, 464 U.S. 417, 442 (1984).

We thank the Copyright Office for initiating this study to address the concerns of copyright owners and users.

## **I. General Effectiveness of Safe Harbors (NOI Questions 1–5)**

### **1. The Problem of Repeat Infringers**

The number of takedown notices sent is staggering, and this number is steadily increasing.<sup>5</sup> As observed by Professor Bruce Boyden,<sup>6</sup>

Even for the largest media companies with the most resources at their disposal, attempting to purge a site of even a fraction of the highest-value content is like trying to bail out an oil tanker with a thimble. . . . The expenses of locating, identifying, and then sending a notice for that many files is so significant that even large companies must limit their efforts.<sup>7</sup>

No one in the notice and takedown ecosystem likes spending time and money to process and respond to millions of takedown notices, when they could be innovating and creating instead. Congress clearly did not intend such outcomes when it passed the DMCA—Section 512 was designed to protect copyrights, to protect non-culpable OSPs from liability when users uploaded infringing files, and to maintain many of the traditional contours of secondary liability in the digital environment.<sup>8</sup> Congress understood that Internet enforcement

---

<sup>5</sup> RIAA alone has noticed 55+ million instances of infringements to websites and 71+ million instances of infringements to search engines. RIAA, *THE DMCA IN 2016: IS IT WORKING?* (2016).

<sup>6</sup> Professor Bruce Boyden is a Professor at Marquette University Law School and a member of the Copyright Alliance Academic Advisory Board.

<sup>7</sup> For data on the quantity of notices sent by the Motion Picture Association of America, see Bruce Boyden, *The Failure of the DMCA Notice and Takedown System: A Twentieth Century Solution for a Twenty-First Century Problem*, CENTER FOR PROTECTION OF INTELL. PROP. (Dec. 5, 2013).

<sup>8</sup> *Columbia Pictures Indus. v. Fung*, 710 F.3d 1020, 1039–40 (9th Cir. 2013) (noting that “the DMCA’s legislative history confirms that Congress intended to provide protection for at least some vicarious and contributory infringement,” and explaining that inquiries into contributory copyright infringement and the prerequisites for one or more of the DMCA safe harbors should be conducted independently); *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993); S. Rep. No. 105-190 at 19, 20 (1998); Boyden, *supra* note 7.

could not be solved unilaterally through government regulations. As noted by Professor Boyden, Congress hoped the law would bring together OSPs and copyright owners to “cooperate to detect and deal with’ infringing sites before content was distributed too widely.”<sup>9</sup>

The safe harbor that Section 512 provides was meant to be a limitation on monetary liability, not an exception to copyright infringement.<sup>10</sup> OSPs were concerned about being party to lawsuits over isolated acts of infringement by their users, even if they were otherwise cooperative in remedying the infringement as soon as they were put on notice.<sup>11</sup> In exchange for OSPs’ cooperation, Congress created “safe harbors” to minimize the possibility that fear of liability would inhibit technological innovation. The bill sought to protect OSPs who work with the copyright community to mitigate and combat online infringement. The inclusion of these safe harbors, along with the other provisions in the bill, allowed the DMCA to “provide greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.”<sup>12</sup> Indeed, a review of the legislative history reveals that the intent of the safe harbors was to afford reasonable immunity to reasonable actors; not to create a mechanism by which OSPs could disregard copyright law.<sup>13</sup>

---

<sup>9</sup> Boyden, *supra* note 7, at 2.

<sup>10</sup> See *Ellison v. Robertson*, 357 F.3d 1072 (9<sup>th</sup> Cir. 2004) *citing* S. Rep. 105–190, at 19 (“Congress provided that ‘limitations of liability apply if the provider is found to be liable under existing principles of law.’”); S. Rep. 105–190 (“The [safe harbor] limitations ... protect qualifying service providers from liability for all *monetary* relief for direct, vicarious and contributory infringement. Monetary relief is defined in subsection [(k)(2)] as encompassing damages, costs, attorneys’ fees, and any other form of monetary payment. These subsections also limit injunctive relief against qualifying service providers to the extent specified in subsection (j).”).

<sup>11</sup> See S. Rep. No. 105-190.

<sup>12</sup> S. Rep. No. 105-190, at 20; H.R. Rep. No. 105-551, pt. 2, at 49-50.

<sup>13</sup> See H.R. Rep. No. 105-551.

Today not only are stakeholders grappling with tens of millions of notices a year,<sup>14</sup> but even worse, the business models employed by certain bad actors actually take advantage of judicial interpretations of this statutory scheme. As a result, uploaders repost infringing content within seconds, and these bad actors profit from having millions of infringing content shuffle off and on of their website. After all, an OSP can obtain revenues even when copyrighted content stays up only for a brief time. If copyrighted content receives just one viewing or download before being taken down, in the aggregate of millions of works, that adds up to millions of ad revenue-producing views for the OSP.<sup>15</sup> Congress did not envision this type of abuse when it enacted the DMCA; such abuse needs to be addressed.

## 2. New Technologies

In 1998, the intent of the notice and takedown process was to give copyright owners a faster alternative to filing for a temporary restraining order in court, mostly so they could keep prevent copies distributed legally on physical goods (DVDs, CDs) from being illegally distributed on the Internet for people to download. Today vastly increased download speeds and instant streaming capabilities have left copyright owners virtually no opportunity to prevent mass unauthorized copying, distribution and performance. Accordingly, automated technologies have become more critical than ever.

Automated technologies can intervene during the upload process, and can simplify the takedown process to effectively shorten the time that infringing content remains available for consumption. While these automated technologies may not work for all service providers, we remain optimistic that investment in new technologies and collaborative agreements are essential to a healthy online ecosystem. Proper interpretation of all of the Section 512 provisions will also incentivize OSPs to invest in automated technologies for copyright owners and their users.

---

<sup>14</sup> Boyden, *supra* note 7.

<sup>15</sup> David Newhoff, THE ILLUSION OF MORE, *Copyright Office to Review Safe Harbor in DMCA* (Jan. 6, 2016), <http://illusionofmore.com/copyright-office-to-review-safe-harbor-in-dmca/>.

### 3. Judicial Interpretation of Section 512

The statutory scheme established by Section 512 goes well beyond the notice and takedown provisions. Courts need to better ensure the requirements set forth in the statute are met: requiring that OSPs have repeat infringer policies; rejecting safe harbor protection for OSPs who directly infringe, or actively encourage or benefit from infringement; and disqualifying OSPs from the safe-harbor immunities when they willfully ignore known infringing content on their websites. OSPs differ greatly in the degree of care they extend to the safe harbor requirements—certain torrent sites, for example, do the bare minimum or disregard the DMCA altogether.

As the Fourth Circuit observed in *ALS Scan. v. RemarQ Comm.*, “[t]he DMCA was enacted both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright infringement liability for ‘passive,’ ‘automatic’ actions in which a service provider’s system engaged through a technological process initiated by another without the knowledge of the service provider.”<sup>16</sup> On the other hand, where an OSP has knowledge of, benefits from, or engages in infringement, the safe harbor is not and should not be available; because their involvement is no longer passive and automatic.

We need to ensure copyright owners—not bad faith OSPs and infringers—are rewarded for their labors and continue to create and disseminate works to the benefit of the public. As such Section 512 requires much more cooperation from OSPs than simply responding to takedown notices.

## II. Notice and Takedown Process (NOI Questions 6-14)

The DMCA notice and takedown process provides a workable legal framework for OSPs and copyright owners to protect against infringement of copyrighted content on the Internet;

---

<sup>16</sup> 239 F.3d 619 (4th Cir. 2001) *citing* H.R. Conf. Rep. No. 105–796, at 72 (1998), *reprinted in* 1998 U.S.C.C.A.N. 649 (“The DMCA’s protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e. at the moment it becomes aware that a third party is using its system to infringe.”).

however, implementation of the process needs to be improved to better respond to highly advanced online infringement tactics and the limited resources of smaller creators and OSPs. Because of the explosion of infringing content online, such improvements should, to the extent reasonable, include the use of automated technologies, even though the occasional so-called “bad notice” may slip through. The vast majority of notices issued by reputable rights owners are legitimate, and the benefits of automated services far outweigh the rare cases of “bad notices.” Also, many larger entities already integrate human review into their automated takedown procedures. But as already articulated, individual creators (who typically have been provided little information and lack meaningful resources) are left to rely on manual web searches, reverse image searches, Google alerts, or word of mouth to discover infringements of their work.

## 1. Individual Creators

We reached out to our individual creator membership to hear their experiences with Section 512’s notice and takedown process. We received 219 responses from creators working in a variety of disciplines.<sup>17</sup> The responses show that (1) many creators do not know how to file a takedown notice or even what the notice and takedown process is; and (2) even if they have participated in the process, they lack access to the technologies necessary to actually keep infringing content from reappearing.<sup>18</sup>

Sixty-eight percent of the creators we surveyed have never filed a takedown notice before because (1) they have either never heard of it; (2) it would take too much effort; (3) the process is too difficult to navigate; or (4) they are skeptical it would do anything to stop online infringement.<sup>19</sup> These are valid concerns, and illustrate a need for easily accessible educational

---

<sup>17</sup> See *infra* Appendix.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*



resources to help creators better understand and avail themselves of the notice and takedown process. These educational offerings will also serve OSPs; better informed copyright owners will ultimately cut down on the number of inappropriate or incomplete notices filed.

Individual creators who file notices lack the resources of larger copyright owners to make a meaningful impact. Eighty-five percent of those we surveyed said they issue takedown notices all by themselves, taking time away from their creative pursuits, which pushes many to give up enforcement efforts all together. These creators are defenseless against the volume and reach of online infringement, especially in light of how easy it is to re-post something nowadays. For example, Keith, a writer from Austin, has never personally posted his work on social media sites, but still spent four hours on Tumblr trying to locate 50 of the 2000+ URLs that contained re-postings of his work: “I can’t afford the time to find the full 2000 [that Tumblr asked for],” he said. He has also found his work on Twitter, Imgur, Reddit, Facebook, Instagram, Pikore, MySpace, Xanga, Nexopia, and more.<sup>20</sup>

And online infringement does not just stop at loss of compensation or control; it also can damage the professional integrity of creators. For example, Melissa, a photographer from California, was horrified to learn that her Victoria Secret style bridal photos were stolen and used on porn sites. “This has been horrible!” she said. “I’ve been in business for 32 years. Married for 35 years and would never create anything for porn!”<sup>21</sup>

Individual creators would benefit from greater access to automated technologies to ease the burden of filing takedown notices. The biggest hurdle is cost: many automated technologies are not yet affordable for the average individual creator, but further discussions of the interested parties could reveal at least some solutions to the problem. Sixty-seven percent of those surveyed still use basic web searching to find instances of infringement and 36% rely, at least partially, on

---

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

word of mouth. Our survey revealed that the only advanced automated technologies at these creators' disposal are reverse image or text searching tools and Google Alerts. More over, the courts can alleviate some of the burden felt by individual creators by properly adhering to the knowledge standards and repeat infringer policies laid out in Section 512. Generally, OSPs (at least the larger entities) are better equipped to implement and extend access to automated technologies than individual creators. Further, as we are already seeing, there is a real incentive to voluntarily provide these tools since doing so simplifies the OSP's existing obligations.

The consensus from our individual creator membership is that online infringement has reached a point where content can be posted on hundreds of online infringement sites within days, and where individual creators—without access to effective tools—are unable to make any real impact in protecting their work. Online infringement has become so commonplace that it destroys once legitimate markets for creators' works. For example, Susan, an audio producer from California, was told by a radio station that they saw no point in paying her for her work because they could “get it for free.”<sup>22</sup>

The impact of online infringement on a creator's livelihood has been thoroughly documented in testimony, news articles, and blog posts over the past few years. Here are just a few of the many stories told by creators:

- Maria Schneider, a Grammy award winning composer, testified before the House Judiciary Committee that she invested \$200,000 of her own money into a new album to only discover her song had quickly been pirated all over the Internet.<sup>23</sup> “The resulting loss of income, combined with the cost of monitoring the Internet and sending takedown notices, threatens her ability to continue creating her award-winning music.”<sup>24</sup>

---

<sup>22</sup> *Id.*

<sup>23</sup> *Section 512 of Title 17: Hearing Before the Subcomm. of Courts, Intell. Prop., and the Internet of the Comm. on the Judiciary* (2014) (statement of Maria Schneider).

<sup>24</sup> *Id.*

- Kathy Wolfe, the owner of the independent film company Wolfe Video, lost \$3 million in revenue in 2012 from the excessive pirating of her top 15 film titles.<sup>25</sup> She “found more than 903,000 links to unauthorized versions of her film” in a single year, spending “over \$30,000 a year—about half of her profits— just to send out takedown notices.”<sup>26</sup> With losses this large, she has been forced to cut her marketing budget in half, cut employees’ pay, and discontinue her own salary.<sup>27</sup> Making art is often expensive, and most artists already sacrifice paying themselves to keep the art going; this should not be exacerbated by online infringement.
- Tor Hanson, co-founder of YepRoc Records/Redeye Distribution, testified in 2013 at the House Judiciary Committee hearing on *Innovation in America: The Role of Copyrights* on this very point: “[We] have limited budgets and whatever revenue and profits [we] can eke out are directed toward [our] primary goals, music creation by [our] music label’s artists and then the marketing and promotion of this music to the American public so they are able to continue this creative process.”<sup>28</sup>

## 2. New technologies and voluntary measures

OSPs and copyright owners alike have voluntarily introduced new technologies that address some of the volume and logistical concerns arising from the notice and takedown process. The documented success of these automated technologies suggest that continued cooperation amongst stakeholders will likely solve many of the other, more complicated problems with administering the law.<sup>29</sup> Partnerships in the technology and copyright sectors will

---

<sup>25</sup> Christopher S. Stewart, *As Pirates Run Rampant, TV Studios Dial Up*, WALL STREET JOURNAL, Mar. 3, 2013.

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*

<sup>28</sup> *Innovation in America: The Role of Copyrights: Hearing Before the Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary*, 113<sup>th</sup> Cong., 6 (2013) (statement of Tor Hansen, Co-President/Co-Founder YepRoc Records/Redeye Distribution).

<sup>29</sup> *Section 512 of Title 17: Hearing Before the Subcomm. of Courts, Intell. Prop., and the Internet of the Comm. on the Judiciary* 75 (2014) (testimony of Katherine Oyama, Sr. Copyright Policy Counsel, Google, Inc.)

lead to smarter, faster, and more efficient automated tools to better identify infringing material without sacrificing user privacy and legitimate fair uses. These partnerships are not only desired, they are critical.

Partnerships will also assist in making automated technologies more accessible. As noted by the composer Maria Schneider, the major concern with these technologies is one of access:

[E]very artist should be entitled to [these] services, to register their music once and for all. Just like the successful ‘do not call list,’ creators should be able to say ‘do not upload.’ If filtering technology can be used to monetize content, it can also be used to protect it ... if you didn’t have Content ID [or similar technologies] for those big companies, I can’t even imagine how big ... takedown numbers would be. They would be insane. So imagine if [automated technologies] worked for everybody.”<sup>30</sup>

This technology may also be useful in identifying works that have previously been taken down to prevent repeat infringements.<sup>31</sup>

#### **a. Content Matching Technologies**

The Google Content ID program, for example, offers qualifying<sup>32</sup> copyright owners access to a fingerprinting program that actively notifies owners of user uploads that contain their material. Google requires a copy of the content in order to place it inside of a database that

---

(“[I]ncentivizing [these] kinds of business partnerships and collaborations so that everyone can kind of grow this pie together and get more content out there with users is the right way to go.”).

<sup>30</sup> *Section 512 of Title 17: Hearing Before the Subcomm. of Courts, Intell. Prop., and the Internet of the Comm. on the Judiciary* 54, 108 (2014) (testimony of Maria Schneider).

<sup>31</sup> Steven Tjoe, *Taking a Whack at the DMCA: The Problem of Continuous Re-Posting*, CENTER FOR PROTECTION OF INTELLECTUAL PROPERTY (Mar. 14, 2014), <http://cpip.gmu.edu/2014/03/14/taking-a-whack-at-the-dmca-the-problem-of-continuous-re-postings/>.

<sup>32</sup> *See generally* YOUTUBE, Qualifying for Content ID, <https://support.google.com/youtube/answer/1311402> (last visited Feb. 9, 2016).

generates a unique fingerprint. Once the fingerprint has been generated, every time a new video is uploaded to YouTube, it will be compared against all the 15 million+<sup>33</sup> fingerprints in its database.<sup>34</sup> Some content owners have chosen to block infringing content, while others have chosen to monetize the content in favor of the copyright owner. The technology underlying the Content ID program is able to identify whether the new upload is an exact or partial copy, and whether the new upload is of lower quality than the original copy (suggesting online infringement).<sup>35</sup> Before participating in the program, copyright owners must prove that they are the lawful and *exclusive* owner of the reference material. Once ownership is established, copyright owners are able to respond to infringing content by either having the content tracked, monetized,<sup>36</sup> muted, or removed. 8,000+ groups have already signed on to the Content ID program, and have claimed over 400 million videos.<sup>37</sup>

Google has also established the Content Verification Program for larger content holders who establish an “ongoing need to have content removed from YouTube” to have advanced searching capabilities.<sup>38</sup> Tools like this are vital to copyright owners who are responsible for large catalogs of works or high-value individual works.

---

<sup>33</sup> *Section 512 of Title 17: Hearing Before the Subcomm. of Courts, Intell. Prop., and the Internet of the Comm. on the Judiciary* 98 (2014) (testimony of Katherine Oyama, Sr. Copyright Policy Counsel, Google, Inc.).

<sup>34</sup> YOUTUBE, How Content ID works, [https://support.google.com/youtube/answer/2797370?hl=en&ref\\_topic=2778544](https://support.google.com/youtube/answer/2797370?hl=en&ref_topic=2778544) (last visited Feb. 9, 2016).

<sup>35</sup> *Id.*

<sup>36</sup> *Section 512 of Title 17: Hearing Before the Subcomm. of Courts, Intell. Prop., and the Internet of the Comm. on the Judiciary* 42 (2014) (testimony of Katherine Oyama, Sr. Copyright Policy Counsel, Google, Inc.) (“ . . . most of our partners are choosing to monetize their content rather than having it all come down.”).

<sup>37</sup> Press Release, YouTube, *Statistics*, <https://www.youtube.com/yt/press/statistics.html>. Part of expanding access to creators is also not excluding those creators who choose to participate in YouTube’s new streaming service from still participating in the Content ID program. See Sandra Aistars, Op-ed: *Why are artists disappearing from the Internet* COPYRIGHT ALLIANCE (June 24, 2014), [http://copyrightalliance.org/2014/06/why\\_are\\_artists\\_disappearing\\_internet#.VrpdeMe9a-8](http://copyrightalliance.org/2014/06/why_are_artists_disappearing_internet#.VrpdeMe9a-8).

<sup>38</sup> YOUTUBE, Content Verification Program Application, [https://www.youtube.com/cvp\\_app](https://www.youtube.com/cvp_app) (last visited Feb. 9, 2016).

### **b. AudibleMagic**

Similar to Content ID, Audible Magic's automatic content recognition technology compares registered content with any attempted video and audio uploads.<sup>39</sup> Embedded into the registered content is the owner's information and any express wishes for how content is to be used.<sup>40</sup> Platforms can then apply this information in conjunction with their own content policies in order to make a timely decision on whether to post the content.<sup>41</sup> At times, the service also leads to direct licensing agreements between copyright owners and platforms.<sup>42</sup> Each month, 250,000 new copyrighted titles are added to the voluminous database of registered content.<sup>43</sup>

### **c. Dropbox Hashtags**

Cloud storage provider Dropbox has developed hashtag technologies (attaching a unique identifier to content) to permit the company to de-duplicate files. According to an article published by TechCrunch, Dropbox stores just one copy of a specific file that can be accessed by any user who has uploaded a copy of that file, saving significant space on Dropbox's server.<sup>44</sup> This same technology is used to save copyright owners the undue burden of having to submit numerous DMCA takedown notices when other parties try to make public the exact same infringing file.

---

<sup>39</sup> AUDIBLE MAGIC, Copyright Compliance Service, <https://www.audiblemagic.com/compliance-service/#how-it-works>.

<sup>40</sup> *Id.*

<sup>41</sup> *Id.*

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> Greg Kumparak, *How Dropbox Knows When You're Sharing Copyrighted Stuff Without Actually Looking at Your Stuff*, TECHCRUNCH (Mar. 30, 2014), <http://techcrunch.com/2014/03/30/how-dropbox-knows-when-youre-sharing-copyrighted-stuff-without-actually-looking-at-your-stuff/>.

#### d. NexGuard Watermarking

AMC Networks, along with other video content owners, has adopted Civolution's NexGuard watermarking technology to deter online infringement of popular TV shows, such as *The Walking Dead*. NexGuard uses session-based watermarking technologies to elevate traditional digital rights management to become more relevant and useful in an international, online environment.<sup>45</sup> A digital watermark is attached to video files, allowing copyright owners to know if any distribution partners leak content before a critical release date.<sup>46</sup> Individual studios have been successful with watermarking to even track individual infringers (by way of set-top boxes), but this technology is largely inaccessible to cable companies, because they would need to "deploy watermark-embedding systems with each pay-TV provider affiliate."<sup>47</sup> Other services providing watermarking technologies for these purposes include Friend MTS and MarkAny.

#### e. Private Sector Voluntary Agreements

In addition to developing new technologies, stakeholders from the Internet ecosystem have developed voluntary agreements to further mutual objectives. Some examples include:

- The TAG initiative, launched in February 2015 validates tools and services that take measures to prevent advertisements from running on pirate sites.<sup>48</sup> According to the Digital Citizens Alliance, ad-

---

<sup>45</sup> *Intertrust Partners with Civolution to Bring NexGuard Watermarking to its ExpressPlay DRM System*, BUSINESS WIRE, <http://www.businesswire.com/news/home/20160217005499/en/Intertrust-Partners-Civolution-Bring-NexGuard-Session-Based-Watermarking>.

<sup>46</sup> Todd Spangler, *Programmer Deploys Civolution's NexGuard watermarks to track source of illegal copies*, VARIETY (Feb. 22, 2016), <http://variety.com/2016/digital/news/amc-piracy-walking-dead-watermarking-1201711621/>.

<sup>47</sup> *Id.*

<sup>48</sup> The Trustworthy Accountability Group (TAG), a coalition of online advertising stakeholders, including advertising agencies, ad placement networks, media companies, and consumer protection organizations. Press Release, Advertising Industry Launches Initiative to Protect Brands Against Piracy Websites, Trustworthy

supported pirate sites can be extraordinarily profitable, with many displaying ads from “blue chip premium brands.”<sup>49</sup>

- The Center for Copyright Information’s (CCI) Copyright Alert System, launched in February 2013, is a partnership between motion picture studios and record labels and five major ISPs to implement a graduated response scheme that uses both educational messaging and mitigating measures to change consumer behavior on transferring illegal files. In the first ten months of operation, 1.3 million alerts were sent, and a CCI study found that 57% of users would stop infringing immediately if they received an alert.<sup>50</sup>
- In 2007, various stakeholders agreed upon the Principles for User Generated Content to eliminate infringing content, while still taking into account fair use considerations. This informal understanding at least illustrates a willingness of OSPs and copyright owners to agree on a middle ground.<sup>51</sup>
- And finally, collaboration between copyright owners and payment processors like Visa, Mastercard, and Paypal—encouraged by the Intellectual Property Enforcement Coordinator—has led to a process that prevents known infringing sites from access to payment networks. This helps cut off the revenues that such sites rely on to operate.

Private-sector voluntary agreements are a critical tool for addressing online infringement.

---

Accountability Group (February 10, 2015), <https://www.tagtoday.net/advertising-industry-launches-initiative-to-protect-brands-against-piracy-websites/>.

<sup>49</sup> DIGITAL CITIZENS ALLIANCE, GOOD MONEY GONE BAD: DIGITAL THIEVES AND THE HIJACKING OF THE ONLINE AD BUSINESS (Infograph) (2014), available at <http://www.digitalcitizensalliance.org/cac/alliance/resources.aspx>.

<sup>50</sup> CENTER FOR COPYRIGHT INFORMATION, COPYRIGHT ALERT SYSTEM: PHASE ONE AND BEYOND 1 (2014).

<sup>51</sup> The agreement was made by CBS, Disney, YouTube, and other copyright owners and OSP entities.



### **3. DMCA Provisions Interpreted Contrary to Congressional Intent**

#### **a. Registered Agent Requirement**

A basic requirement of an OSP receiving the Section 512(c) safe harbor is designating an agent with the U.S. Copyright Office to receive notifications of infringement. This requirement also mandates that an OSP list the agent's contact information on their website, and that they set up email forwarding to ensure notifications are not being sent to outdated email addresses.<sup>52</sup> The importance of this requirement was evident in the Ninth Circuit decision *Ellison v. Roberts*, in which the court denied AOL the benefits of the Section 512(a) safe harbor after it failed to direct communications to a proper registered agent. AOL did not forward emails from its old email address to its new one.<sup>53</sup> This essentially created a "vacuum" for notices of infringement to fall into and be ignored.

Our membership has experienced numerous instances of absent or inaccurate information regarding an OSP's designated agent, making enforcement difficult or impossible to follow through on. For these reasons, OSPs seeking the safe harbors must keep accurate their registered agent information. This problem could be rectified in part with a modernized Copyright Office. For example, an improved IT system might allow the Office to test the accuracy of the contact information listed in its designated agent directory, and to put in place a simpler system for OSPs to update their contact information.

#### **b. Representative List**

The DMCA notice and takedown process, as often interpreted by the courts, has largely placed the burden on copyright owners to list every instances of infringement on an OSP's

---

<sup>52</sup> 17 U.S.C § 512(c)(3) (2012).

<sup>53</sup> 357 F.3d at 1080 (9th Cir. 2004) (noting that while AOL did update its address with the Copyright Office, its failure to forward emails left some takedown notices fully ignored).

website. The “representative list” requirement in provision 512(c)(3)(A)(ii) specifies that a takedown notice must identify the “copyrighted work claimed to be infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a *representative list* of such works at that site.” This is paramount, given the volume of online infringement, because creators too often lack the time, money, and resources to list with specificity every single URL containing infringing copies of their work. Notwithstanding this language, the courts have recently begun placing the sole burden of tracking, identifying, and “adequately documenting” infringements squarely on the copyright owner, which makes little sense in practice and discourages individual creators from enforcing their rights.<sup>54</sup>

Congress did not intend this high degree of specificity for notices. As noted in the legislative history, the “representative list” requirement is satisfied,

[f]or example, where a party is operating an unauthorized Internet jukebox from a particular site, it is not necessary that the notification list every musical composition or sound recording that has been, may have been, or could be infringed at that site. Instead it is sufficient for the copyright owner to provide the service provider with a *representative list* of those compositions or recordings in order that the service provider can understand the nature and scope of the infringement being claimed.<sup>55</sup>

### **c. Information Location Tools**

This NOI asks whether Section 512(d), covering “information location tools” such as search engines, appropriately addresses OSPs that link or refer to infringing content. When the DMCA was drafted, search engines already played a significant role in the Internet ecosystem. In the years following its enactment, that role grew exponentially. Today when someone is looking for something on the Internet, the first place they go to is a search engine. While search engines

---

<sup>54</sup> See *Perfect 10 v. CCBill*, 488 F.3d 1102, 1113 (2007); *Viacom Int’l v. YouTube, Inc.*, 940 F.Supp. 2d 110, 115 (S.D.N.Y. 2013).

<sup>55</sup> H.R. Report No. 105–551 (emphasis added).

often direct people to lawful sources of content, too often they also direct users to illegal content. It is imperative that OSPs who provide information location tools and copyright owners find ways to work together to effectively address these infringement problems.

While the copyright community appreciates many of the additional steps these OSPs have taken, it is important that the steps be effective and not just symbolic. For example, Google has implemented a policy whereby it demotes sites based on the number of takedown notices that Google receives in conjunction with other factors. Unfortunately, the demotion policies, and other policies, have largely been ineffective because infringing content still shows up near the top of search results. One solution would be for search engines to place less weight on the infringing site's traffic and more weight on the number of takedown notices the site receives. Another solution would be for OSPs and copyright owners to jointly enlist the support of independent third parties to evaluate the effectiveness of particular measures, develop ways to improve their efficiency and effectiveness, and to highlight best practices.

#### **4. Human Review and Bad Faith Notices**

The vast majority of notices are sent in good faith. In the rare circumstance where a copyright owner sends a notice in "bad faith," the counter notification procedure offers an adequate remedy.<sup>56</sup> Additionally, as stated by Professor Sean O'Connor, even many of the notices sent are simply repeats of previously taken down content:

The highest volume of notices seem to be for reposted works, i.e., ones that have already been taken down on notice, yet reappear within hours often on the same site. Further, many of these do not even purport to be transformative or non-infringing. They are not mash-ups, remixes, covers, etc. They are simply the original work reposted repeatedly by an unauthorized person. That the posters do not seem to believe they have any real rights to the works seems

---

<sup>56</sup> See 17 U.S.C. § 512(g) (2012).

supported by the surprisingly low number of counter notices submitted (relative to the enormous number of takedown notices).<sup>57</sup>

Our members are ardent supporters of fair use. As creators, our members often rely on fair use in their own work. The automated tools mentioned previously typically only remove infringing content that is between a 90–100% match of the reference file submitted by the copyright owner.<sup>58</sup> As one observer noted, “Targeting these egregious cases makes sense given that the continuous re-posting of blatantly (really, inarguably) infringing wholesale copies accounts for the vast majority of takedown notices.”<sup>59</sup> Creators are overwhelmed by how much clearly infringing content is available on the Internet. Generally creators tend to only issue takedown notices for the most egregious cases. It is unlikely that a takedown notice would be issued for a use that may be reasonably construed as fair.

### III. Counter Notices (NOI Questions 15-18)

The counter notification process ensures that users uploading content have a mechanism for responding to notices sent by mistake or in bad faith. The challenge, however, lies in the range of options available to a copyright owner in those circumstances where a counter notice is filed improperly. The Act provides that the copyright owner has only ten days to bring suit against the alleged infringer, otherwise the infringing material or link is re-posted.<sup>60</sup> Bringing a federal lawsuit is a significant burden, especially for individual creators; and the ten-day requirement is, as a practical matter, virtually impossible to satisfy for even the larger, more

---

<sup>57</sup> *Section 512 of Title 17 Hearing Before the Subcomm. Of Courts, Intell. Prop., and the Internet of the Comm. on the Judiciary* 14 (2014) (testimony of Sean O’Connor).

<sup>58</sup> Even Electronic Frontier Foundation has supported certain automated technologies. *Fair Use Principles for User Generated Video Content*, ELECTRONIC FRONTIER FOUNDATION (“[f]iltering mechanism is able to verify that the content has previously been removed pursuant to an undisputed DMCA takedown notice or that there are ‘three strikes’ against it ... [including] nearly the entirety (e.g. 90% or more) of the challenged content is comprised of a single copyrighted work.”).

<sup>59</sup> Tjoe, *supra* note 31.

<sup>60</sup> 17 U.S.C. § 512(g)(2)(C).

sophisticated copyright owners. Making matters worse, in some circuits a copyright owner must first receive a copyright registration certificate (as opposed to simply registering their work) in order to bring an infringement case; this adds to the burden on smaller copyright owners.<sup>61</sup> If the copyright owner has not registered the work before sending the takedown notice, there is no way they could meet the ten-day requirement—even if they apply for expedited registration.<sup>62</sup>

Although many OSPs have attempted to educate their users about the counter notification process, very few counter notices are ever filed; the content targeted by most takedown requests is almost always clearly infringing, or is posted by users who do not wish to reveal their identity or location. A number of OSPs have developed educational material to make the counter notice process easier for their users to understand.

#### **IV. Legal Standards (NOI Questions 19–21)**

In a world where online infringement is so routine and pervasive, the courts must stop condoning improper OSP takedown policies.

##### **1. The Red Flag Standard**

An OSP will lose safe harbor protection by failing to act when confronted with actual or apparent knowledge. Copyright owners can provide the OSP with actual knowledge by sending a notice, or they can prove the OSP has apparent knowledge<sup>63</sup> of infringement under the “red flag

---

<sup>61</sup> See, e.g., *La Resolana Architects, PA v. Clay Realtors Angel Fire*, 416 F.3d 1195, 1202-07 (10th Cir. 2005), *abrogated on other grounds by Reed Elsevier v. Muchnick*, 559 U.S. 154 (2010); *M.G.B. Homes, Inc. v. Ameron Homes, Inc.*, 903 F.2d 1486, 1488-89 (11th Cir. 1990), *abrogated on other grounds by Reed Elsevier*, 559 U.S. 154 (2010).

<sup>62</sup> Due to staffing and other resource challenges, the Office’s current pendency times for applications now exceed a year for certain registrations. See *F.A.Q.*, COPYRIGHT OFFICE, <http://copyright.gov/help/faq/faq-what.html#certificate> (noting that paper applications can take up to 13 months; electronic applications up to eight).

<sup>63</sup> 17 U.S.C. § 512(c)(1)(A)(ii) (“red flag knowledge”).

knowledge” standard.<sup>64</sup> Once aware, the OSP is required to “act expeditiously to remove, or disable access to, the material” to remain safe harbor protections.<sup>65</sup>

Under the red flag knowledge standard, a copyright owner can prove an OSP has knowledge by showing it was aware of facts or circumstances that make infringement apparent. The court asks whether (1) the OSP was aware of the circumstances of infringement (the so-called “subjective prong”); and (2) the “infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances” (the so-called “objective prong”).<sup>66</sup> However, the Second Circuit in *Viacom v. YouTube*<sup>67</sup> and the Ninth Circuit in *UMG Recordings v. Shelter Capital Partners*<sup>68</sup> arguably made the OSPs only responsible for responding to the infringement explicitly identified in takedown notices.<sup>69</sup> These courts’ interpretation of the red flag standard is so restrictive that it has basically eliminated the carefully balanced burden allocation that Congress intended. It would be helpful if the Copyright Office would offer guidance to courts to help them more accurately interpret the provision going forward.

## 2. Willful Blindness

Additionally, some courts have incorrectly applied the concept of willful blindness in the safe harbor context. Knowledge of infringing activity will be imputed to an OSP who has consciously avoided obtaining actual knowledge under a theory of willful blindness.<sup>70</sup> In *Viacom*

---

<sup>64</sup> H.R. Rep. No. 105–551 (II), pt. 2, at 58 (1998).

<sup>65</sup> 17 U.S.C. 512(e)(1)(A)(iii).

<sup>66</sup> H.R. Rep. 105–551, pt. 2, 61 (1998).

<sup>67</sup> 676 F.3d 19 (2d Cir. 2012).

<sup>68</sup> 106 U.S.P.Q.2d 1253 (9th Cir. 2013).

<sup>69</sup> See Boyden, *supra* note 7.

<sup>70</sup> *Viacom*, 676 F.3d at 35 (quoting *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 109 (2d Cir. 2010)).

*v. YouTube*, the Second Circuit correctly articulated that willful blindness is triggered when the OSP is “aware of a high probability of the fact [of infringement] and consciously avoid[s] confirming that fact.”<sup>71</sup> The willful blindness doctrine provides courts with additional guidance and effectuates Congress's intent to “discourage today’s common ‘do not look’ policy,”<sup>72</sup> and to encourage the sorts of advanced “trust and safety” departments that are implemented by groups like eBay.<sup>73</sup> But in *Capitol Records v. Vimeo*, the court shielded the OSP from liability despite a record that showed the OSP and its employees turned a blind eye to infringement. The court determined that any conscious avoidance by the OSP needs to be “tailored” to the “specific infringing content at issue in the litigation,” and that the knowledge demonstrated in the record “did not relate to the Videos-in-Suit.”<sup>74</sup> However, the hallmark of a willfully blind defendant is that the defendant has affirmatively avoided acquiring specific knowledge about infringing material or activity on its system. By definition, then, a service provider that is willfully blind to infringing activity on its system has ensured that it will not have knowledge that is “tailored to” the “specific infringing content at issue,” because that is the very knowledge the service provider has consciously avoided.

As a practical matter, if improper lower court decisions like these continue to proliferate, OSPs will effectively have no affirmative obligations. Congress envisioned the DMCA as creating a regime of joint responsibility, in which OSPs would act reasonably and proactively in the face of actual or apparent knowledge. Coupled with the existing practical limitations of the notice and takedown process, copyright owners would have little meaningful protection against

---

<sup>71</sup> 676 F.3d 19 (2d Cir. 2012).

<sup>72</sup> Tjoe, *supra* note 31.

<sup>73</sup> eBay voluntarily spent as much \$20 million per year to promote trust and safety on its website; set up a “trust and safety” department with 4000 employees, over 200 of which were dedicated solely to deterring infringement; implemented a “fraud engine” as early as 2002 in order to ferret out illegal listings; and canceled certain transactions. *Tiffany Inc.*, 600 F.3d 93.

<sup>74</sup> *Vimeo*, 972 F. Supp. 2d at 524–25.

online infringement. When there is no meaningful “red flag” knowledge requirement, the result is a toothless statute. The Copyright Office should articulate to the courts that many of these decisions are misinterpreting the knowledge standards, and by doing so, are disregarding the legislative intent behind drafting them in the first place.

## V. Repeat Infringers (NOI Questions 22–23)

To be eligible for the safe harbor, an OSP must design and implement a sufficient repeat infringer policy. OSPs are not required to police their sites for infringements, so long as they have reasonably<sup>75</sup> implemented a repeat infringer policy; however, the courts will decline to protect an OSP under the safe harbor provisions when they have actual knowledge of a user’s “blatant, repeat infringement of a willful and commercial nature.”<sup>76</sup> Congress wanted to ensure that infringers “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.”<sup>77</sup>

We want to be clear that repeat infringer policies are “fundamental safeguard[s] for copyright owners ... essential to maintain[ing] the strong incentives for [OSP]s to prevent their services from becoming safe havens or conduits for known repeat copyright infringers.”<sup>78</sup>

---

<sup>75</sup> *BMG Rights Mgmt, LLC v. Cox Communication*, 2015 U.S. Dist. LEXIS 161091 (V.E.D.C. 2015) (citing *CCBill LLC*, 488 F.3d at 1109); *Capital Records, LLC v. Escape Media Grp., Inc.*, No. 12-cv-6646, 2015 U.S. Dist. LEXIS 38007, 2015 WL 1402049, at \*9 (S.D.N.Y. March 25, 2015) (“For example, a service provider must have a ‘working notification system’ and a ‘a procedure for dealing with DMCA-compliant notifications,’ and the provider must ‘not actively prevent copyright owners from collecting information needed to issue such notifications’... Additionally, the penalty imposed for repeat infringers (when appropriate circumstances exist) must be termination and not some lesser consequence.”).

<sup>76</sup> *Corbis v. Amazon*, 351 F. Supp.2d at 1104; *CCBill*, 488 F.3d at 1102.

<sup>77</sup> H.R. Rep. 105–551, pt. 2, 61 (1998).

<sup>78</sup> *Capitol Records, Inc v. MP3Tunes, LLC*, 821 F.Supp.2d 627, 637 (S.D.N.Y. 2011).



The problem is not in the legal framework drafted by Congress, but instead in how OSPs choose to implement policies. As illustrated in *Capitol Records v. Escape*, some OSPs are fully capable of identifying works and tracking repeat infringers, but instead choose to craft a repeat infringer policy in a way that makes enforcement nonexistent.<sup>79</sup> As the court found, the online music service provider Grooveshark, owned by Escape, had two policies for removing content: One Strike and DMCA Lite.<sup>80</sup> Under the One Strike policy, content would be removed and the user would be banned from re-posting content.<sup>81</sup> On the other hand, under the DMCA Lite policy—which made up 94% of all Grooveshark takedowns—any takedown notice that Grooveshark decided did not perfectly comply with the DMCA’s requirements would only result in the content being removed, the user’s account would remain active.<sup>82</sup> In denying Grooveshark immunity under the safe harbor, the court noted that “[a]dopting a repeat infringer policy and then purposely eviscerating any hope that such a policy could ever be carried out is not an ‘implementation’ as required by § 512(i).”<sup>83</sup> Yet because Grooveshark publicly claimed it complied with the DMCA (even though it did not) it was able to operate for 8 years.<sup>84</sup> For nearly a decade, Grooveshark profited from massive copyright infringement, misled users into thinking that they were a legitimate music service, and competed unfairly with other legitimate and licensed music services.

---

<sup>79</sup> Copy L. Rep. (CCH) P30, 744 (S.D.N.Y. 2015).

<sup>80</sup> *Id.*

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*

<sup>83</sup> *Id.*

<sup>84</sup> Letter from Paul Geller, Grooveshark’s Executive Vice President (“There does appear to be some confusion about whether Grooveshark is a legal service. So let’s set the record straight: there is nothing illegal about what Grooveshark offers to consumers. . . . First, there is a distinction between legal and licensed. Laws from Congress. Licenses come from businesses. Grooveshark is completely legal because we comply with the laws passed by Congress, but we are not licensed by every label (yet). We are a technology company, and we operate within the boundaries of the Digital Millennium Copyright Act of 1998.”) Digital Music News has since removed the open letter from their website.

Through cooperation, OSP should be able to adopt more acceptable repeat infringer policies. Some progress has already been made in this regard by multi-stakeholder groups such as the Center for Copyright Information with its Copyright Alert System program. The Department of Commerce’s Internet Policy Task Force has voiced support for this graduated alert system; which tracks a subscriber’s frequency of infringing activity, and imposes elevating consequences for continued activity.<sup>85</sup> Such efforts should be expanded to include other stakeholders and additional categories of creative works.

## **VI. Standard Technical Measures (NOI Questions 24–25)**

As new automated technologies advance and receive the approval of relevant stakeholders, these groups should work together to ensure these technologies meet the requirements of “standard technical measures” (STMs) under provision 512(i). This is a statutory device made even more important in light of provision 512(m), which states that an OSP has no duty to monitor for infringements “except to the extent consistent with a standard technical measure complying with the provisions of subsection (i).”<sup>86</sup> So, failing to accommodate an STM would disqualify an OSP for the safe harbor, thereby subjecting them to liability.<sup>87</sup>

Utilizing this entirely un-utilized statutory device would permit parties to enter into voluntary agreements without need for new enforcement provisions in the Act itself. After all, Congress strongly “urge[d] all of the affected parties expeditiously to commence voluntary, inter-industry discussions to agree upon and implement the best technological solutions available to achieve these goals.”<sup>88</sup>

---

<sup>85</sup> INTERNET POLICY TASK FORCE, COPYRIGHT POLICY, CREATIVITY, AND INNOVATION IN THE DIGITAL ECONOMY 2 (2010).

<sup>86</sup> 17 U.S.C. § 512(m)(1).

<sup>87</sup> *Viacom*, 676 F.3d at 41.

As written, there is enormous potential for the STM provision to incentivize new technologies and encourage stakeholder collaboration. However, to satisfy the requirements of the statute, stakeholders would need to come together “in an open, fair, voluntary, multi-industry standards process.”<sup>89</sup> Further, any agreements should make applicable STMs also available to individual creators, and in a way that does not overly burden OSPs. It seems whatever obstacles may exist do not relate to finding entities willing to voluntarily create automated technologies—that is already happening—but rather, the extent to which stakeholders can come together in a timely process to make those tools publicly available. The Administration’s Intellectual Property Enforcement Coordinator and the Copyright Office could look at the experience of the Department of Commerce’s Internet Policy Task Force’s DMCA multi-stakeholder process to inform its own approach to these issues.

## **VII. Remedies (NOI Questions 26–28)**

### **1. Misrepresentation**

Provision 512(f) applies misrepresentation claims under a subjective standard, placing the burden on the alleged infringer to show that the copyright holder believed that the content subject to its takedown notice was non-infringing. In *Rossi v. Motion Picture Ass’n of America*, the Ninth Circuit articulated,

[w]hen enacting the DMCA, Congress could have easily incorporated an objective standard of reasonableness. The fact that it did not do so indicates an intent to adhere to the subjective standard traditionally associated with a good faith requirement ... Congress included an expressly limited cause of action for improper infringement notifications, imposing liability only if the copyright owner’s notification is a “knowing misrepresentation. A copyright owner cannot be liable simply because an unknowing mistake is made, even if the copyright owner acted unreasonably in making the mistake. Rather, there must be a demonstration of some

---

<sup>89</sup> 17 U.S.C. § 512(i)(2)(A).

actual knowledge of misrepresentation on the part of the copyright owner.<sup>90</sup>

Copyright owners already bear the burden for enforcing their copyrights on the Internet, so if there were legislative changes to expand 512(f), it would potentially open these owners up to “limitless lawsuits just [for] policing [their] copyrighted material on the Internet.”<sup>91</sup> The Copyright Office should confirm that misrepresentation claims should be analyzed under the subjective good faith standard. As discussed previously, the overwhelming majority of takedown notices are legitimate; lowering the threshold for what is considered an illegitimate notice, or increasing penalties would severely undermine the statutory scheme with little positive benefit. To the extent that provision 512(f) does not do enough to address abusive takedown notices, voluntary best practices are the most appropriate vehicle for improvement.

## **Conclusion**

The Copyright Alliance and its members embrace technologies that give creators new platforms to disseminate their work; however, these users of these technologies should also respect creators’ exclusive rights. The notice and takedown process was meant to provide an efficient mechanism for addressing online infringement, but it can only be effective if the other interrelated requirements of Section 512 remain meaningful and effective. Stakeholders must come together, as Congress intended, to sculpt lasting principles that establish boundaries that creators, innovators, and OSPs should all respect.

---

<sup>90</sup> 391 F.3d 1000, 1004–05 (9th Cir. 2004), *cert denied*, 544 U.S. 1018 (2005).

<sup>91</sup> *Ouellette v. Viacom Int’l, Inc.*, No. CV-10-133-M-DWM-JCL, slip op. (D. Mon. Mar. 13, 2012).

If you have any questions or would like any additional information regarding our views in this submission, please contact Sarah A. Howes at [showes@copyrightalliance.org](mailto:showes@copyrightalliance.org).

Respectfully submitted,

Keith Kupferschmid  
Chief Executive Officer & President  
Copyright Alliance  
1224 M Street, NW, Suite 101  
Washington, D.C., 20005

## Appendix

### The Copyright Alliance Survey

#### Individual Creators Thoughts on the DMCA Notice and Takedown Process

- The DMCA takedown process affects all kinds of creators, but most of our feedback came from visual artists; such as photographers and illustrators.

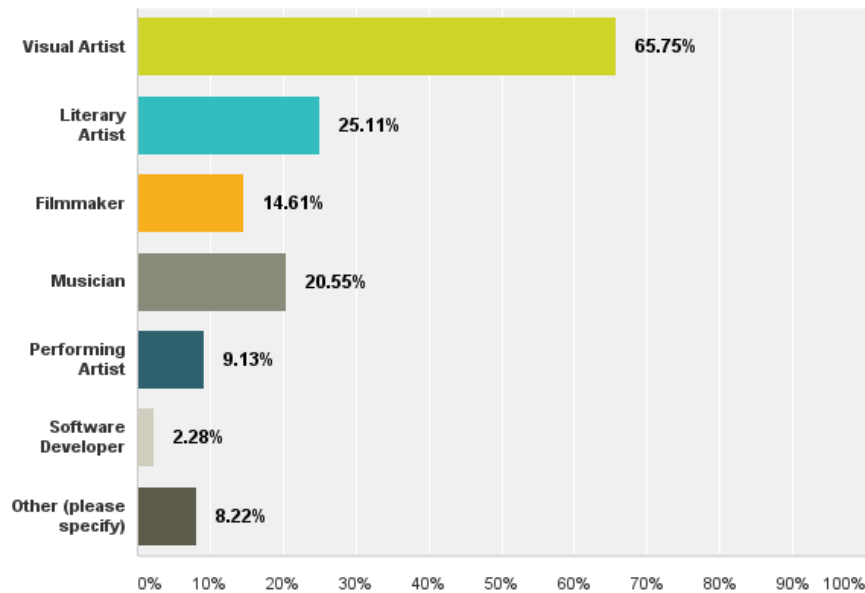


Figure 1 Who Participated in Our Survey

- 126 (59%) of the 213 participants have been directly harmed by online piracy, and many offered concrete examples of how piracy has cost them money, time, and business:
  - “Piracy has ruined the music industry and everyone’s career who has anything to do with it. In addition to losing work, I can’t get a proper recording contract, because labels no longer have development capital for unknown artists.” – John, Musician, San Francisco, CA
  - “People scan my photos from old books & magazines and post them online. There is a huge amount of time involved in fighting this piracy.” – Charlyn, Photographer, New York City, NY

- “About 10% of my content has been stolen, repackaged, and re-sold by third parties on the Internet” – James, Filmmaker, Carlsbad, CA
- “I have lost tens of thousands of dollars to online piracy” – Romeo, Filmmaker, South Pasadena, CA
- “A stolen image is later stolen by another website, and another, creating a long steam of infringements. Each usage should have a fair fee. Issuing a takedown notice would be fine, but it’s at a volume for photographers that it would take not only days but weeks. None of the infringements I’ve experienced would have merited a formal lawsuit, as the groups taking my work are small-scale entities. I do not want a lawsuit, I do want fair payment for each use.” – Hillary, Photographer, Oshkosh, WI
- “I am a freelancer and I rely on selling each story to make money. A local radio station takes my stories out of a statewide show and uses it as though I did the story for them. They refuse to take freelance stories from me, because they say they can “get it for free.” – Susan, Audio Producer/Reporter, Lomita, CA
- “My last film was pirated almost immediately after it’s digital release, and within days was available on over 100 piracy sites.” – Tom, Filmmaker, Oak Park, CA
- “I have no way of knowing how many pirated copies of my books have been downloaded. I used to spend hours sending DMCA notices, but after I noticed that oftentimes the books were re-loaded, I gave up. It’s not possible to estimate what I’ve lost.” – Carol, Writer, Wellesley, MA
- “My work has been pirated numerous times, and DMCA’s are not always effective. Even if the sites take the content down, usually it’s back up again in a few days. Some sites make it so difficult to find the way to contact them to send a DMCA in the first place that it’s next to impossible. Some require so much personal information, which is then used to harass the content creator, that it’s safer to not contact them at all.” My sales are very low anyway, and it hurts knowing that my work is out there for free, with little recourse to do anything about it.” – Michele, Writer, Olympia, WA

- “I sent Tumblr a takedown notice with a URL and some text, and asked them to take down the URL and all the 2000+ re-blogs that accompanied that post. After 4 hours, I had URLs for 50 of them. I can’t afford the time to find the full 2000. I have never posted on any social media site, but my work has been posted unlawfully on Twitter, Tumblr, Imgur, Reddit, Facebook, Instagram, Pikore, MySpace, Xanga, Nexopia, and many more.” – Keith, Writer, Austin, TX
  
- “We used to be able to make a living from music production and album sales. This has almost completely disappeared. The day our latest album was released it was immediately available on various pirate sites. Google searches ranked those pirate download links first, at the top of the first page of search results, above our own web site and legitimate stores.” – Zenon, Musician, New York
  
- “Someone stole photos from a private link to a client and posted them on a porn site. This is an ongoing problem now. I had taken glamor/bridal boudoir photos of my bride to give her new husband as a gift. The photos were Victoria Secret type. Not X rated. However, it came to my knowledge that the link to the photos was shared by the hacker. This has been horrible! I’ve been in business for 32 years. Married for 35 years and would never create anything for porn! Not to mention my client’s privacy being breached.” – Melissa, Photographer, Santa Barbara, CA
  
- When asked, 68% (a significant majority) of creators surveyed said they have never filed a DMCA takedown notice.

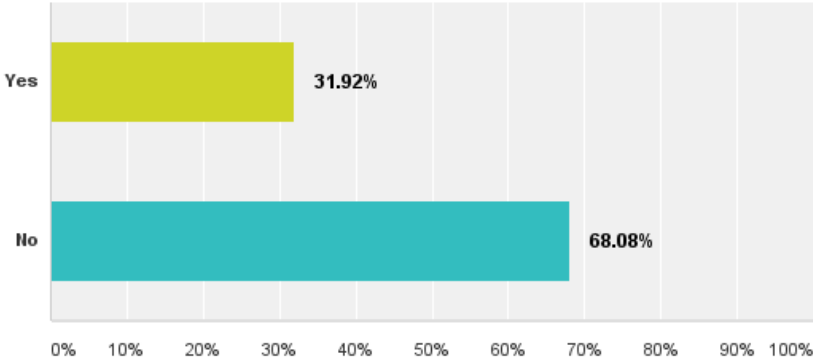
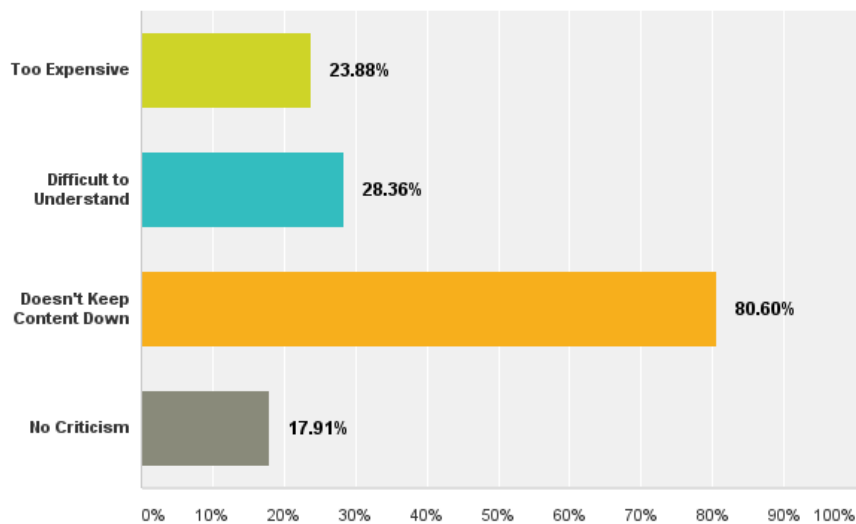


Figure 2 Do Creators File DMCA Takedown Notices?

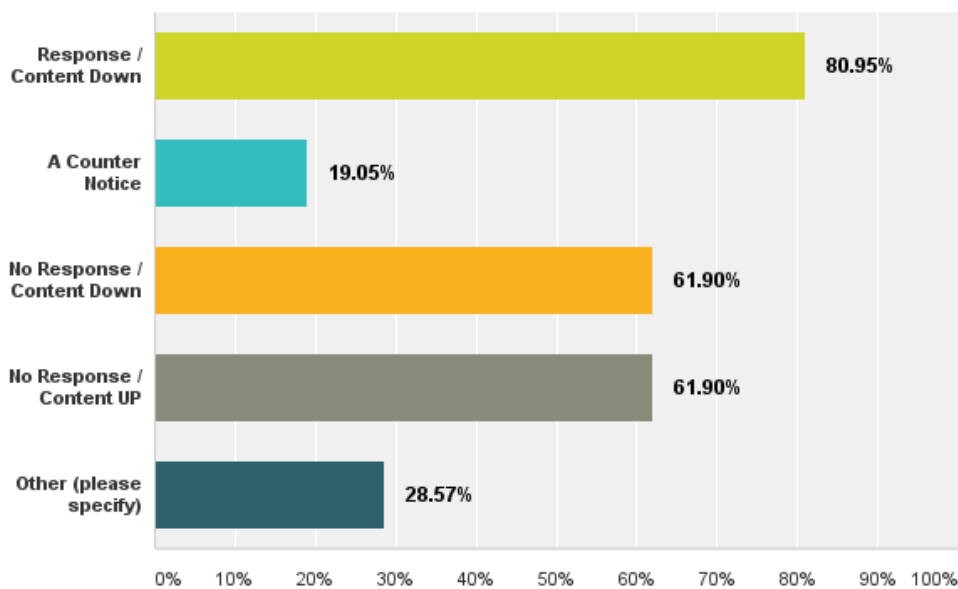


- Of those who have never filed a DMCA takedown notice:
  - **42%** said they've never heard of the process before;
  - **14%** said it was too much effort to try to understand;
  - **12%** said the process was too difficult to navigate;
  - **20%** they were too skeptical a notice would do anything; and
  - **22%** of those surveyed said they've never had their work infringed on the Internet.
- For those creators who have filed a DMCA takedown notice, they found the notice and takedown process ineffective, because it:



- When asked who files notices on the creator's behalf, **85%** responded that they file the notice themselves, without the help of staff, an attorney, a third-party service.
- When asked what tools or methods do creators use to discover infringing content on the Internet:
  - **67%** said they conduct manual web searches;
  - **36%** said they find out from word of mouth;
  - **31.75%** said they use reverse image services like TinEye or Pixsy; and
  - **11.12%** said they use at least one of the following methods: name, title or text tracking, watermarking, or the Google Alert service

- As evidenced by our survey responses, not every notice sent resulted in a response from the OSP that the content had been taken down. Creators were free to select as many answers that applied to their experiences. **61.9%** of creators who answered this question said they had at least one instance of not receiving a response from the OSP and the content itself just staying up. This question does not even touch on the fact that even if content is initially taken down, it often goes right back up again.



- For those **28.5%** creators who choose “other,” the stories were most unfortunate. Creators received:
  - Hostile comments or online bullying;
  - Threatening messages that argued the OSP was legally justified in keeping content up;
  - Runarounds where the OSP claimed the notice was not specific enough, or that the creator had to prove their identity; or
  - Bounce emails or error messages that the notice did not process.