March 31, 2016

United States Copyright Office
Section 512 Study Comment Submission

Section 512 Study on safe harbors
Comments by the International Association of Scientific Technical and Medical Publishers (STM)

Dear Sirs

The International Association of Scientific Technical and Medical Publishers (STM) welcomes this opportunity to submit comments in the Section 512 Study.

STM is the leading global trade association for academic and professional publishers. It has over 120 members in 21 countries who each year collectively publish nearly 66% of all journal articles and tens of thousands of monographs and reference works, including many members who are either based or have places of business in the United States. STM members include learned societies, university presses, private companies, new starts and established players. The primary interest of STM and its members lies in published works intended for the academic and research markets.

In this submission, we would like to focus on the experiences of our members in applying notice and takedowns against hosts of content stored at the direction of the users of the host's service, as meant in Section 512(c) of the Digital Millennium Copyright Act ("DMCA"). These comments are in answer to the following questions in the Notice of Inquiry:

General Effectiveness of Safe Harbors
1. Are the section 512 safe harbors working as Congress intended?
2. Have courts properly construed the entities and activities covered by the section 512 safe harbors?
4. How have section 512's limitations on liability for online service providers impacted the protection and value of copyrighted works, including licensing markets for such works?
5. Do the section 512 safe harbors strike the correct balance between copyright owners and online service providers?

Notice-and-Takedown Process
6. How effective is section 512's notice-and-takedown process for addressing online infringement?

7. How efficient or burdensome is section 512's notice-and-takedown process for addressing online infringement? Is it a workable solution over the long run?
8. In what ways does the process work differently for individuals, small-scale entities, and/or large-scale entities that are sending and/or receiving takedown notices?
10. Does the notice-and-takedown process sufficiently address the reappearance of infringing material previously removed by a service provider in response to a notice? If not, what should be done to address this concern?

Structurally infringing websites

The experience of many STM members has been that there are content hosting web sites which create business and operational models to work around the provisions of Section 512, enabling them to claim entitlement to "safe harbor" protection from liability even while incentivizing copyright infringement on a massive scale. These hosting sites are commonly referred to as "structural infringers" because, while their technology is "content neutral" and they generally comply with DMCA takedown notices to claim refuge in the 512(c) safe harbor, their businesses are blatantly structured to encourage an ongoing supply of journals and books published by STM's members without authorization and in a way that infringes their copyrights. These structural infringers also facilitate the infringing supply of all kinds of other copyright works, including music and movies.

One type of structural infringer is the so-called "cyberlocker." Some cyberlocker sites reward anonymous users who upload copyrighted content to the site for access by other anonymous users all over the world. The rewards are based on the popularity of the content, measured by how many visitors download it or how many premium memberships are sold because of it. Visitors to these sites seek copies of high quality movies, books, music and other copyrighted content. Advertising income and subscription fees are usually their sole revenue sources. As a result, they reap substantial profits from the content they exploit without having to invest a single dollar to develop, create, or publish it.

When an artist or rights holder sends a takedown notice, the structurally infringing site usually removes or disables the specific infringing material or link, which entitles the site to the DMCA safe harbor from monetary liability if the site also meets other statutory criteria. The original uploader or some other user, however, often re-uploads the same work to the site, or the file itself is not removed, only the specific link, leaving other links to the file available. In this way, rights holders seeking to enforce their copyrights by way of Section 512, end up in a "whack-a-mole" situation. (For a full analysis of the conduct of cyberlockers and a comparative analysis of the applicable notice and takedown provisions in the United States and Europe, see "Distinguishing Common Carriers from Common Thieves" by Paul Doda in the upcoming *Journal of the Copyright Society of the USA*, Vol. 63 No. 3.)

By issuing appropriate injunctive relief, US Courts could require sites to take reasonable measures to prevent the serial re-uploading of previously removed works, identified by the relative (often numerous) DMCA takedown notices. Injunctive relief can prevent structurally infringing host sites from continuing to undermine the DMCA's goals and takedown mechanisms.

Supplementary measures should be considered to require host sites that have already removed infringing content to prevent the re-uploading of identical infringing content, for example by:

1. Preventing the re-use of an identical URL to host the same infringing content.
2. Filtering for identical infringing files by using a file hash, or other identifiers or metadata identified from the originally infringing file.
3. Providing immediate takedown mechanisms / tools to trusted rights owners to remove files in respect of which they have already previously served notices.

Content delivery networks that mask structurally infringing websites

A content delivery network or content distribution network (CDN) is a globally distributed network of proxy servers deployed in multiple data centers. CDNs are a relatively recent innovation and the infringement issues associated with them post-date the original DMCA legislation.

The goal of a CDN is to serve content to end-users with high availability and high performance. The CDN is not the ultimate host of the infringing content, but its service may obscure who the ultimate host actually is. For instance, an IP address lookup on a website using a CDN's services will return an IP address for the CDN instead of the IP address of the site where the content is actually being hosted.

A takedown notice issued to a CDN will not result in blocking access to the content nor obligate its client to remove it – this is despite the CDN being aware of the infringement and arguably facilitating it by delivering the content on behalf of its client. The CDN may forward the take down notice to its client and its host, notify the complainant that it has done so, and also inform the complainant who the underlying host is. If a host site which delivers its pages via the CDN and is in receipt of our notice fails to remove the infringing content, then the CDN takes no further action. Furthermore, if the client moves its hosting server (for whatever reason, voluntarily or involuntarily), then the complainant does not get to know about it unless it serves an additional notice to the CDN and receives the new host's name.

Obfuscating the IP address and host of CDN clients makes the DMCA process harder and therefore more expensive. If a rights owner then chooses to escalate by litigating, he may not know for some time whether a host has changed, which then in turn disrupts the legal process.

Section 512 could be improved by clearly including CDNs as service providers that are subject to DMCA notices, and covered by the safe harbor provisions relating to these. As an available form of injunctive relief issued by a court, a CDN should be obligated to stop domain routing to infringing sites if the site and/or its ISP fails to comply with a DMCA notice. CDNs should also be obligated to give rights owners (rather than just the hosts of infringing content) the true underlying IP addresses of infringing sites if the site and/or its ISP has failed to comply with a DMCA notice, or, at the very least, pursuant to DMCA a 512(h) subpoena.

Problematic takedown notice requirements imposed by notice recipients

Many sites that host infringing content insist that DMCA notices are sent via dedicated web reporting forms, others by way of application process interfaces (APIs). Some have even completely stopped accepting email notices.

Some of the web reporting forms are non-standardized, are often updated without warning, often do not work at all or experience downtime, and have varied and complex "captcha" and "hints" security checks which limit automation of notice sending.

The quantity of notices which can be sent via web forms also varies from site and/or host. Some allow multiple notices, whereas there are others which allow notice of just one infringement per form submission which - when one considers all the checks to go through before submitting - makes the reporting of thousands of infringements on the most egregious sites impossible. Other sites/hosts/services limit how often one can submit a notice to the same URL – which makes submitting notices very impractical, in particular on sites which use CDN services (see above).

Book related piracy sites often have a 'read-on-line' functionality in that each page of an online book has a different URL. This means that, if the book displayed is an infringement, the DMCA notice has to list a separate URL for each page in order to get the whole book removed. When applied to some of the cases of web reporting forms referred to above, a rights holder could potentially have to send a separate notice for every page.

The need by some sites for dedicated API mechanisms for DMCA notices is understood, especially for cases where high volumes of reporting are anticipated. However, the formats of APIs vary greatly from site to site and the lack of standardization results in unnecessary burdens in cost and effort for rights holders.

The DMCA should expressly disallow websites claiming safe harbor protection from prescribing the method in which DMCA notices are delivered to them. (For supplementary suggestion on availability of email addresses to receive notices, see below.) It must be expressly mandated that an email address for the submission of DMCA notices must always be available.

Privacy and proxy domain registration impediments

The many privacy and proxy services available that enable domain owners to register their domains anonymously are a practical impediment to delivery of DMCA notices. Currently the only way to get the contact information behind a proxy service is to apply for a court order, which is a complex and costly process.

Email addresses for receipt of DMCA notices

Sometimes it is difficult to determine what the correct email address is for the serving of notices, which is further complicated if the email address changes.

An industry standard could be considered for the email address prefix for the serving of all DMCA notices e.g. “dmca@[domain].com”.

We thank you for this opportunity to contribute to the Section 512 Study and we would be pleased to assist you in your further deliberations.

Yours faithfully,

Michael Mabe
Chief Executive Officer
STM, International Association of Scientific, Technical and Medical Publishers
mabe@stm-assoc.org