



455 Massachusetts Ave., NW
Suite 700
Washington, D.C. 20001
Telephone: (202) 347-3375
Fax: (202) 347-3690

December 10, 2010

**Comments of the
Association of American Publishers
in Response to the
Department of Commerce
“Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy”
[Docket No. 100910448–0448–01]**

Introduction

The Association of American Publishers is the national trade association of the U.S. book and journal publishing industry. AAP’s some 300 members include most of the major commercial publishers in the United States, as well as smaller and non-profit publishers, university presses, and scholarly societies. AAP members publish hardcover and paperback books in every field, educational materials for the elementary, secondary, postsecondary, and professional markets, scholarly journals, computer software, and electronic products and services. The protection of intellectual property rights in all media, the defense of the freedom to read and the freedom to publish at home and abroad, and the promotion of reading and literacy are among the Association’s highest priorities.

The AAP and its membership appreciate the opportunity to provide its views on this important subject. We note that while a great deal of government attention has been given to how online piracy has affected the music and movie industries, online piracy is very much a problem for all content industries – including the book and journal publishing industry.

To organize our Comments, we have taken the liberty of conflating the numerous questions in the Notice into a list of topics and subtopics which encompass the Department’s questions. Our responses appear immediately below each topic heading and subheading.

Category 1: Rightsholders – Protection & Detection Strategies for Online Infringement

Rightsholder Experience with Online Copyright Piracy:

- Technologies used to engage in online copyright piracy

At any given moment, massive numbers of books, journals, and other copyrighted text-based products are freely and anonymously shared by individuals throughout the world through various online sources, in blatant violation of the copyright owners’ rights, and to the detriment of everyone in the value chain for the creation and legal dissemination of

content. The sources include file-hosting sites (“cyberlockers” or “one-click hosting” sites) featuring infringements which are then widely posted on blogs, forums, and other websites; file search (“indexing”) sites; and publicly-available peer-to-peer networks (“P2P”) that are engaged in widespread infringement of copyright. In many instances the sites may be outside the reach of U.S. law. As the Department of Commerce’s Internet Policy Task Force (the “Task Force”) heard during its listening sessions, misuse of cyberlockers has become an increasingly vexing issue for rights holders. This is especially true for the publishing industry as text-based files are relatively small and are easily made available via direct downloads from cyberlockers, which generally provide infringers with greater anonymity compared to distributed file-sharing methods such as the BitTorrent protocol.

While operators of file-sharing sites reap ill-gotten profits from the operation of the sites, the remedies available to the publishing industry (and other content owners) are not adequate to address the problem effectively. These commercial piracy sites use well-known financial transaction services and feature advertising from reputable companies. Traffic to these sites is often driven by the promise of free content. Publishers continually learn of online sites, often based outside the U.S., which are offering significant numbers of infringing electronic files of their copyrighted products for download. These services popularize their domain names to promote traffic on the site, and in a large number of instances derive revenue from sales of subscriptions to their entire “library” of pirated works, sales of downloads of the pirated files on an individual or bulk basis, and/or sales of advertising space on the site. Such sites will typically accept payments through major credit card companies or through other payment services such as PayPal. Advertisers run the gamut of products and services, and include many well-known companies that are probably not aware that their brands are being associated with, and indeed supporting, piracy. Some sites even operate as sham “not for profit” entities seeking charitable contributions (which may be donated through PayPal, for example) to enable the site to continue to offer infringing content for free.

- Prevalence, economic effects, and substitution rate assumptions of such piracy

A number of studies have attempted to measure the volume of infringing materials available online but there has been, to our knowledge, no comprehensive study to date that seeks to directly measure actual losses attributable to online book and journal piracy.

Establishing an accurate substitution rate has been difficult. In past studies where an estimated “loss” value has been ascribed to those instances of online piracy that it was possible to track in the study, the multiplier used has either been the value of the pirated product at pirate price – in which case, the estimated loss likely substantially underestimates the harm to industry – or, the legitimate price which, it is argued, overestimates the loss due to online piracy. Whatever substitution rate is used, it is particularly difficult to establish volume, given the lack of data that websites engaged in trafficking infringing content are willing to provide. For example, currently it is usually not possible to determine how many times a file that has been uploaded to a cyberlocker has been downloaded.¹ This is a key piece of data needed to establish an accurate estimate of loss.

¹ A few of the major sites listed this information in the past, but discontinued doing so after the monitoring vendor Attributor used the data in its report on downloading activities discussed on page 4 of these Comments.

With the advent of tablet devices and the increase in legitimate e-book downloads, it can be surmised that substitution rates are on an upward trajectory and that the correct loss value is increasingly the legitimate e-book price.

AAP points out that while it recognizes the utility of arriving at even an estimated loss value, the volume of infringing material found online is sufficient to establish that content owners face a severe problem and that far stronger measures are necessary to aid rights holders in combating large-scale online infringement.

While establishing lost sales figures is rather elusive due to a lack of in-depth information regarding the purchasing behavior of illegal downloaders, as well as the issue of what methodology to apply to arrive at a calculation, publishers have in at least several instances observed strong evidence of direct, negative effects on the sales of particular products as a consequence of documented instances of piracy in either digital or print form. There is even a report where the publisher was eventually able to achieve a significant reduction in the number of available infringements of a particular textbook online through sustained takedown efforts over a multiyear period, and in turn saw a correspondingly dramatic increase in its sales of units of the book.²

Publishers suspect that sales losses due to piracy are especially significant in the case of professional reference materials, though circumstantial evidence is often hard to come by since these materials are usually traded privately (such as via e-mail). The research service Outsell, Inc. issued a report in February on sharing behaviors among corporate, healthcare, government, and education workers. It estimated a nearly six-fold increase in unauthorized sharing of copyright-protected works since 2005. The findings were based on a Web-based survey conducted in September 2009. More than 50% of the respondents either did not think about copyright before sharing, or were ambivalent about it. Methods of sharing included sending attachments, links, or embedded texts through e-mail; photocopying; and a variety of other means. Another problem publishers are facing involving unauthorized sharing is the surreptitious misuse or theft, and subsequent trading and sharing, of login credentials for access to publishers' entire online databases licensed to academic institutions. In addition to the potential for enabling large-scale piracy, this unauthorized access compromises the legitimate accounts of major institutions whose credentials are misused or stolen.

There is also concern that digital piracy will eventually stymie what is currently a flourishing trade (i.e., general-interest fiction and non-fiction) e-books marketplace. Two years ago, e-books were believed to account for only around 1% of trade book sales revenues. That number has now increased to nearly 9% among trade publishers reporting this information³. As e-book reading devices grow in popularity, the threat of pirated versions substituting for legitimate sales will grow significantly. The increased use of tablet computers is likely to contribute to this trend and will likely affect magazines and other periodicals as well as e-books.

- Observations, if any, regarding patterns of online infringement as broadband Internet access has become more available

² We would be happy to put Department of Commerce officials in touch with the relevant publishers for the details regarding their tracing of specific, measureable lost sales resulting from the availability and downloading or other copying of pirated versions of the works.

³ http://publishers.org/main/PressCenter/Archives/2010_Dec/AAPReportsOctoberBookSales.htm.

There is a direct correlation between an increase in broadband penetration and adoption and increases in the amount of online infringing behavior. This is due to faster upload and download times, coupled with technologies designed to facilitate increased transfer speeds.

A study conducted by the monitoring service Attributor in the last quarter of 2009 documented that more than 9 million downloads were made of infringing electronic versions of 913 copyrighted books from U.S. publishers which were tracked. (The study is available online at http://www.attributor.com/docs/Attributor_Book_Anti-Piracy_Research_Findings.pdf). Journals and other products are being illegally shared on many of the same sites where pirated books are appearing. It should be noted that this study only tracked a small number of total titles available from the U.S. book publishing industry, which published more than 288,000 book titles in 2009 (for more information please visit <http://bowker.com/index.php/press-releases/616-bowker-reports-traditional-us-book-production-flat-in-2009>).

Also, AAP members include both large and small to medium-sized publishers. Many of the smaller publishers do not have the resources to engage in the ongoing monitoring and takedown demand notification process required by the DMCA. The escalating pressure on these companies from online piracy significantly threatens not only the U.S. Gross Domestic Product and exports, but also our society and culture in immeasurable ways. If new approaches are not made possible to stem the rising tide of digital piracy, society will undoubtedly be substantially harmed as creativity, the provision of quality, peer-reviewed information and thinking, and the professional and well-edited presentation of stories, information, and instruction erode away.

A subsequent Attributor study⁴ concluded that online searches for pirated books increased by 50% from August 2009 to September 2010, and that a 20% increase occurred from May 2010 – when Apple’s iPad device became widely available – to September 2010.

Publishers will be better able to gauge piracy activity and industry losses, and to improve how they allocate antipiracy resources, if ISPs begin providing data including how many downloads have been made of the infringing files detected on their servers.

Detection/Prevention of Online Infringement:

- Effectiveness of technologies used to detect/prevent online infringement, and incentives to encourage use by ISPs and payment service providers

Automated web crawlers are being used by rights holders to identify infringing content. While these crawlers are generally capable of locating links to copyrighted works that are listed on various third-party indexing sites, without referring to the indexing sites the crawlers would be incapable of identifying the underlying hosted infringing files that are contained on the cyberlockers and peer-to-peer networks themselves. This lack of transparency not only prevents rights holders from knowing the percentage of the infringing versus non-infringing material on the sites, but also allows re-listing of infringing materials over and over again – thus forcing rights holders to engage in an

⁴ Results and an executive summary are available at the following links: <http://attributor.com/blog/a-first-look-at-demand-for-pirated-e-books-across-the-web> and http://www.attributor.com/docs/BookResearch_Attributor_October2010.pdf.

ineffective and wasteful “whack-a-mole” process to protect their valuable intellectual property against repeat infringers.

Filtering technologies can prevent clearly-identifiable or previously-identified infringing content from appearing and reappearing, but have yet to be adopted by most ISPs. Publishers strongly advocate having websites filter to detect infringing content and to prevent it from appearing (and reappearing) on the site, as described in the “Principles and Best Practices for File-Sharing Websites and Services” promulgated by AAP (attached as “Exhibit A”). Two popular file-hosting sites – Scribd.com and Wattpad.com – have deployed technical filters which reportedly have achieved dramatic drops in the number of infringements appearing on the sites, in turn reducing the numbers of instances where publishers need to send takedown notices to the site operators. (Scribd uses a database of full and partial texts of works which the publishers have flagged as copyright protected and not authorized to be shared, against which its filter checks the content of all files users attempt to upload to the service. Wattpad’s system checks the uploads against a database which identifies publishers’ products by author name, publisher and imprint name, and the title of the product.)

Encryption or other “Digital Rights Management” technologies are often used by publishers in an effort to track or prevent unauthorized access to or reproduction of their products. These technologies can be a critical component of publishing companies’ copyright protection and enforcement strategies, and have incentivized many publishers to make an extensive array of digital products available. As some consumers of trade (i.e., general interest) books have raised concerns regarding difficulties they have encountered with DRM-enabled and protected products, trade book publishers have beefed up their customer-service staffing to help consumers legitimately access content they have purchased (such as by helping customers navigate the technology).

However, pirates have developed a number of ways to get around DRM protection. We should note that even hard copy materials are not safe from digital piracy. Infringers simply tear the cover off the printed version of a book, use a sheet-feeding scanner to digitize its content, clean up spelling errors and formatting, and make the infringing version available online in one or more popular digital formats. Such groups are prevalent in Asia and represent a serious threat to U.S. and European publishers. One specific group which repeatedly appears in anecdotal contexts is Team LIB, which posts links to pirated digitized books on a variety of one-click hosting and indexing sites. There are also third-party services that will create PDF scans of books for a fee (please see www.blueleaf-book-scanning.com, and http://www.huffingtonpost.com/hack-college/how-to-digitize-your-text_b_730879.html). With respect to DRM-protected materials, hackers frequently strip the technical protections off publishers’ digital products. Furthermore, production files are often leaked onto the Internet – such as by an unscrupulous employee of a third party vendor providing format conversion or other production services to the publisher – in many cases resulting in the availability of a product prior to its authorized release.

Technology solutions show great promise to address the problem of massive copyright infringement. However, the sites have to be willing to adopt these solutions. When a site has a business model based on making infringing content available, it will not be willing to adopt these technologies, because doing so would undermine its business model. For this reason, content industries look to courts in other countries, such as Germany, where the requirement to adopt technology solutions is viewed as a practical and effective solution to protect the rights holder’s interests.

Rights holders are willing to work with ISPs and other technology solutions providers to develop effective technologies. In addition to ISP cooperation in adopting technology solutions, AAP urges ISP cooperation in working with rights holders to address repeat infringing behavior. Both technology solutions and remedies to address repeat infringers are critical to countering the significant harm occurring as a result of digital piracy.

- Effectiveness of litigation as an option for preventing Internet piracy

Earlier this year, six of the largest publishers of educational materials in the U.S. brought a successful copyright infringement lawsuit in Germany against the file-sharing service RapidShare (a cyberlocker). In February, a Hamburg court issued a preliminary injunction requiring RapidShare to prevent continuing piracy on its site of 148 books that were the subject of the action. Notwithstanding the injunction, a number of the works continue to appear on the RapidShare site, and the publishers have had to file two separate actions for administrative fines. This month, the Regional Court of Hamburg upheld the imposition of a fine of 150,000 euros against RapidShare for its failure to comply with the injunction.

RapidShare claims that one-third of its paying users are business clients sharing legal content (please see the last bullet point on page six of the presentation at http://www.siia.net/piracy/workshop/Rapidshare_Raimer.pdf), but has not explained the nature of the remaining two-thirds of its subscribers, a vast number whom appear to be copyright infringers.

While actions in Germany have been successful, the publishers are well aware that litigation is not a sufficient tool, especially considering several major case decisions by U.S. Courts in recent years. Unfortunately, these cases have cut strongly against the ability of content-based industries to protect their products against infringement by sites which have knowledge that they are making a large amount of infringing content publicly available and yet take no proactive steps (e.g., filtering, etc.) to mitigate piracy, but only respond to specific takedown notices sent to them by rights holders over and over again.⁵

As a long-term strategy, litigation is neither expeditious nor cost-effective. It places a huge burden upon rights holders – in terms of legal costs and additional personnel necessary to police the web for infringing content – and likewise, harms consumers as rights holders inevitably need to divert funds better spent for research and development to further innovate their products to instead pursuing willful infringers.

Litigation spearheaded by the U.S.-based Evangelical Christian Publishers Association (ECPA) is illustrative of this problem. In 2003, the ECPA became aware through two of

⁵ Most recently, in *Viacom v. YouTube*, a federal judge misconstrued the DMCA's safe harbor provisions for Internet service providers to blur the distinction that Congress sought to make between those entities that might occasionally unknowingly transmit, store, or link to infringing content versus those that knowingly make infringing content available online as an attractive draw to grow their businesses. The court ruled that, absent "knowledge of specific and identifiable infringements of particular individual items," awareness of "a generalized practice of infringement . . . or of a proclivity of users to post infringing materials" does not impose responsibility on service providers "to discover which of their users' postings infringe a copyright." In practical terms, this view encourages service providers to turn a blind eye toward infringement on their systems, with the assurance that they will be protected from liability as long as they comply with statutory takedown notices by promptly removing infringing material that is identified by copyright owners. (2010 U.S. Dist. Lexis 62829)

its member publishers of a web site at www.biblecentre.net, which featured a collection of the full texts of hundreds of copyrighted Christian theological works displayed without permission.

The site first offered free access to the texts, and then charged a subscription fee. ECPA persuaded the hosting ISP to shut down the site, only to see it reappear on a different ISP. This began a seven-year process of shutting down the site on approximately ten ISPs in seven different countries around the world. An ECPA-led coalition of seven publishers brought legal action in December 2007 in the United Kingdom against the owner of the site (the Defendant), securing a court order in March 2008 requiring shut down of the site. After a brief period, the site reappeared at a new URL and the Defendant went into hiding for over a year.

When a private investigator finally found the Defendant in June of 2009, the Defendant claimed that he had transferred ownership of the site to an organization in China and was therefore no longer responsible for the continued infringement. The publishers hired a digital forensics expert to prove the Defendant was still managing the site remotely, and then filed a contempt of court application in December 2009. The Defendant again went into hiding and refused to appear at the hearing. The UK court issued a warrant for his arrest. Under pressure of additional legal penalties, the Defendant eventually shut down the site, appeared in court, and a consent order was entered to resolve the infringement. The Defendant was deemed judgment proof due to lack of financial resources. As a result, the publishers bore all of the considerable expense to take action against the egregious infringement.

Currently there is no viable legal process in the U.S. for pursuing the leading infringement sites. Under the current state of U.S. law, it would be extremely difficult to mount a successful copyright infringement claim against some of the sites featuring the largest numbers of digital infringements of publishers' products. For example, certain high-volume cyberlocker sites are at least responsive to DMCA takedown notices. However, following a take down, the infringing material quickly re-appears on the site under a different URL. In addition, cyberlocker sites often have some legitimate, non-infringing material available, though it may be minimal. So long as U.S. law immunizes these sites, no matter how much money the sites are making off downloads of infringing material, publishers' hands are tied. In contrast, courts in Germany have recognized the need for RapidShare to take more proactive steps to cease hosting specified infringing content, rather than just addressing individual instances of infringement (i.e., specific URLs) on a per-notice basis. In addition, many rogue infringement sites are located outside the U.S., and establishing jurisdiction can be problematic.

Even if publishers were to obtain jurisdiction and a favorable decision in a copyright infringement action against a foreign website, there may be no practical remedy available. Absent the ability to have Internet Service Providers either block the website or stop providing service to it, publishers must live with the infringing material remaining available for download in the U.S.

Another impediment is that typically, domain name registrars are unwilling to enforce their terms and conditions regarding misuse of a domain name, which deprives rights holders of a simple and effective enforcement mechanism. Technology interests should also recognize their own stake in strengthening online enforcement, since it is the content traversing the Internet which drives user activity and traffic.

The lack of remedies for content owners under U.S. law sends a rather negative message to other countries around the world about the importance of protecting the copyrights of U.S.-based authors and publishers. As the world leader in exports of copyrighted products, the U.S. should be taking the lead in ensuring the protection of copyright in the digital environment. We do, however, applaud the recent announcement by the U.S. Immigration and Customs Enforcement (ICE) of the seizure of the domain names of numerous piracy sites pursuant to existing seizure provisions in the U.S. Code (<http://www.ice.gov/news/releases/1011/101129washington.htm>). These actions convey the appropriate message that the U.S. government has a keen interest in protecting the rights of copyright owners and their ability to continue to produce high quality content and goods.

Business Models and Online Copyright Piracy:

- Challenges in developing new business models to offer content online and counteract infringing downloads and streaming.

Despite challenges brought by online piracy, rights holders continue to take risks and invest in developing new business models that provide consumers with greater access to a greater variety of content – as and when they desire to access such content. Some textbook publishers have begun publishing their digital content as part of Web-based services that offer “learning and assessment” approaches to the traditional classroom experience. However, even in these circumstances, piracy of textual and test materials is possible and does occur.

The ability of rights holders to continue to invest in developing new business models will be negatively affected by the need to divert funds to pursuing willful infringers. This will necessarily have an adverse effect on the quality of investment made by rights holders in further enhancing technologies that make delivery of content more efficient and thereby enhance the consumer experience.

- Most-likely-to-succeed online business models and how IP laws and government policies can promote their success and discourage infringement-driven models while respecting fair use and the exchange of non-copyrighted information online.

As long as business models exist which are based on making infringing content available for free and in violation of the copyright owners’ rights, there will not be a level playing field that will allow for true innovation – creative original innovation – to fully thrive. Businesses like RapidShare have succeeded because they offer free content, a free-for-all of copyright theft – and users have flocked to the site. If sites were precluded from offering content belonging to others, they would be forced to develop truly innovative ways to attract users.

As discussed below, under “Rightsholder Experience with Collaborative Approaches,” best practices will need to clearly identify the roles and responsibilities of all parties which have a stake in the online economy, including through IP laws and government policies which demand that sites take reasonable, proactive steps including filtering, effective repeat infringer policies, and other means to remove from their sites infringing content that they can reasonably identify. These measures would obligate sites to rely on having legitimate content to be profitable, while providing a strong disincentive for sites to rely on business models built around pirated content.

An argument made by some individuals who oppose – or even ridicule – copyright holders’ seeking to enforce their rights online is that authors and publishers must either radically change their business models, or go out of business. Putting aside the fact that our industry now offers more than two million e-book titles, a vast array of electronic journals, digitally-based textbooks and other educational products, and the ability of customers to opt to purchase portions of their choosing of many e-book products in lieu of the whole work, detractors contend that authors and publishers must transition further to models in which the works which they publish are no longer relied upon as a primary revenue source, but instead are used to drive ancillary businesses such as providing public speaking or conference services for a fee. While there are indeed a finite number of authors and publishers for whom these services are a significant source of revenue, that is not in any way a reasonable basis for concluding that the entire book and journals industry, or even a substantial portion of it, could viably convert to this model. Moreover, the argument completely ignores the Intellectual Property Clause of the U.S. Constitution empowering Congress “To promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.” (Please see http://www.archives.gov/exhibits/charters/constitution_transcript.html).

Category 2: Internet Intermediaries – Safe Harbors and Responsibilities

Rightsholder Experience with Takedown Notices:

- Volume of takedown notices across different types of online services

AAP’s members include not only the largest publishers of trade (general interest fiction and nonfiction), educational, and professional books, journals, and other works in the U.S., but also many smaller and medium-sized publishers serving the same markets. Several AAP members have provided data on their takedown notification efforts, which we provide below. To supply the Department of Commerce with the information it has requested, we have maintained the anonymity of our member companies and simply designated the data source as “Publisher A,” Publisher “B,” etc. We would be happy to put relevant Department of Commerce officials in touch with the individual publishers who submitted the data if so requested. It should be noted that while the data reported by the publishers includes numbers of infringements found and takedown notices sent, the publishers do not have data on the numbers of times each of these files were downloaded. As discussed on page 4 of these comments, Attributor’s study released in January indicated dramatic numbers of downloads with respect to the 913 titles on which it collected this information: an average of approximately 10,000 downloads of each individual title.

Publisher A

- Number of takedown notices (“TDNs”) sent to ISPs since August 2009: 29,771
- Fees paid to third-party monitoring vendor: More than \$100,000 annually.
- Staff members working on monitoring and takedown efforts as well: One and a half people full-time, plus 20% of a senior executive’s time.

Publisher B

- Number of takedown notices/actions to date in 2010: 73,472
- Fees paid to third-party monitoring vendors so far in 2010: \$126,000

Publisher C

- Number of infringements found from July 2009-present: 21,653

- Costs to engage in the monitoring and takedown efforts, including fees to third-party monitoring vendor: More than \$50,000

Publisher D

- Infringements found in 2009: 15,401
- Fees paid to third-party monitoring vendor for 2009: More than \$91,000
- Infringements found from January through September of 2010: 14,727
- Fees paid to third-party monitoring vendor so far for 2010: More than \$74,000

Publisher E

- Number of infringements found from April 2007-June 2009: 75,421
- Number of infringements found from August 2009-Sep. 2010: 37,776
- In addition to using third party monitoring and takedown vendors, has two full-time staff members designated to preparing and sending takedown notices in response to infringements on websites, file-sharing services, and peer-to-peer networks.
- Also has several other staff members shouldering some of the additional takedown notice generation and sending.

Publisher F

- Cumulative number of infringements taken down from websites and peer-to-peer networks in June, July, and September of 2010: 11,700

Publisher G

- Based on pilot monitoring and takedown notification with respect 500 selected titles, the publisher estimates the existence of a total of 336,000 infringements across its entire list of works.

Publisher H

- Number of takedown notices on infringements of 50 book titles over a recent two-month period: 132
- Takedown notices sent from April through October 2010: 123 TDNs to cyberlocker sites, and 96 TDNs to indexing sites.

Publisher I

- Number of infringements found on cyberlockers during the past 10 months with the help of a monitoring vendor: 1,900 in the first month, and approximately 100 per month since then.
- Fees paid to third-party monitoring vendor over the 10-month period: approximately \$2,500 per month.
- Staff members working on monitoring and takedown efforts as well: 4, spending a total of approximately 30 hours per week altogether.

Publisher J

- Number of takedown notices/actions in 2009: 44,703
- Number of takedown notices/actions so far in 2010: 29,931
- Fees paid to third-party monitoring vendor: Since January 2008, a minimum of approximately \$5,000 per month. From February 2007 to October 2010, approximately \$213,220.
- Staff members working on antipiracy as well: One full-time antipiracy specialist, plus an additional four to five people each spending about 25% of their time on enforcement against online piracy.

Publisher K

- Has used a third-party monitoring vendor since April 2010.
- Fees paid to the vendor to date: \$90,000
- Number of infringements found/takedown notices sent to date: 1,251.
- Staff members dedicated to monitoring for and preventing infringements: 100% of one staff members' time, and part of three additional staff members' time.

Publisher L

- Using two different vendors and on its own, takedown notices covering 300 books and journals since May of 2009: 16,000
- Fees paid to monitoring vendors: more than \$100,000.

This means that among just ten U.S. publishers (listed as Publishers A, B, C, D, E, F, I, J, K, and L), more than 299,000 available online files infringing their copyrighted products have been detected within the past two years alone; among just eight of the publishers (Publishers A, B, C, D, I, J, K, and L), a total of more than \$776,000 has been paid to third-party monitoring vendors within the past two years; and among only five publishers (Publishers A, E, I, J, and K), a total of more than seven full-time staff persons' hours are currently being dedicated to takedown efforts. All of these totals are very conservative representations – a large majority of the publishers only monitored for a portion of the period from 2009 to the present, and the aggregated staff hours figure does not include time spent by staff who work part-time on takedown efforts, but for whom the publisher did not specify a particular number of hours or percentage of the person's schedule in its reporting to AAP. Furthermore, while the aggregated numbers for infringements found, monies spent on third-party vendors, and staff hours devoted to takedown efforts are quite substantial, they represent only a handful of the more than 2,824 publishers publishing books in the U.S., according to the U.S. Census Bureau (please see http://factfinder.census.gov/servlet/IBQTable?_bm=y&-geo_id=&-ds_name=EC0751SSSZ3&-lang=en). The U.S. ISBN agency R.R. Bowker, which includes small publishers in its count, lists a much higher number of active U.S. publishers: more than 250,000 in the current year (<http://www.bowker.com/index.php/component/content/article/29>). We submit that when Congress passed the DMCA, it did not contemplate a financial and administrative burden on rights holders to generate takedown notices and police for repeated infringements at anywhere near the levels we are now seeing them having to contend with.

Currently a handful of the largest file-hosting sites (including RapidShare.com, 4Shared.com, Depositfiles.com, Megaupload.com, and others) account for a large majority of the infringing electronic versions of AAP members' products available online. Stopping the piracy on these sites and increasing the consequences and penalties for all sites systematically engaged in making infringing content available would have a demonstrable and significant positive impact.

- Processes employed to identify infringers in order to send takedown notices

Some of the larger publishers have dedicated staff continuously monitoring for infringements of their companies' products online and sending takedown notices to sites containing infringements and to their ISP hosts. The experience varies widely, however. Monitoring services report compliance with takedown notices by locker sites, although it is impossible to tell how long files have been illicitly posted before the monitoring service locates them and sends a notice. At the other end of the spectrum, however, a number of sites fail to comply with takedown notices, and some even state explicitly on their site that they will not comply.

AAP has entered into an arrangement with the Publishers Association (P.A.) in the U.K. to enable our members to subscribe on an annual-fee basis to use the Copyright Infringement Portal service that was created by the P.A. to help publishers serve takedown notices and keep track of compliance. Publishers who subscribe can enter the Web address “URLs” where they have independently located infringements of their products, and the portal automatically generates takedown notices to the applicable ISP, addressed to the agents assigned by the ISPs to receive infringement notices.

Many publishers are also hiring vendors at significant costs to conduct monitoring and send takedown notices for them on an ongoing basis. These vendors typically use automated crawlers that search for infringing files that have been uploaded to cyberlockers and shared on blogs, forums, and other websites, as well as for links to infringing files that are indexed on Torrent indexing sites. This activity is akin to an expensive game of “whack-a-mole,” treating the symptom rather than the source of the problem, which is the existence of sites that enable copyright infringements to take place without substantial financial consequences and redress. Unfortunately, thousands of new infringements of the publishers’ content come online all the time despite these efforts and expenditures.

- Timeliness of responses to takedown notices

Some sites respond quickly to takedown notices, but merely responding to repeated takedown notices is not sufficient in the current environment. A better recourse is to enable proactive content filtering as users upload files, as this reduced the burden for both rights holders and site operators. There are reportedly some sites that already employ such technology.

- Challenges of managing system of takedown notices

Cyber locker sites: Given the volume of infringing material available on cyber locker/one-click-hosting sites (such as RapidShare), sending takedown notices has become an increasingly burdensome and inefficient measure through which to address online infringements occurring through such sites. Many of these sites do not allow keyword searches, so publishers are reduced to acting upon third-party anecdotal reports of illicit postings or looking for links that appear on third-party indexing or other sites, rather than systematic searches on the site itself.

Cyber locker sites should have more than just a responsibility to respond on a per-notice-received basis. They should have the responsibility to put proactive filtering in place to ensure that copyrighted material is not uploaded, and they should bear the cost of doing so. Rights holders continue to shoulder a tremendous burden in not only policing the Internet for infringing behavior and content but also in notifying ISPs of the volume of infringing material available on their site. At a minimum, cyberlockers should be encouraged to provide rights holders with administrative access to remove infringing files directly. Some sites already do so, but more need to follow suit.

In many instances, such sites *having already received a multitude of notices of infringement – from a great many rights holders – are already well aware of the nature of the majority of the content available on their sites.* To insist that a notice must be sent for every instance of infringing content ignores this fact and thereby sanctions a site’s “turning a blind eye” to unlawful conduct, indeed, arguably a site’s willful negligence. This significant problem begs the question of whether it was the intention of Congress,

and of foreign legislatures, that the safe harbor provisions for Online Service Providers under the DMCA and comparable statutes abroad be an open-ended “get out of jail free” card for the online service providers.

Rightsholder Experience with Systematic (and Repeat) Infringers:

- Challenges in identifying such infringers:

Infringers as ISPs: Systematic infringers who operate their own websites typically operate under a variety of names, URLs, and domain names, so that even identifying them is difficult.

Infringers as users of a cyberlocker, website, or P2P network: There is also a significant challenge in identifying systematic and repeat infringers who upload unauthorized content to cyberlockers.⁶ The issue is that it generally is not possible to identify users who upload infringing content to cyberlockers without subpoenaing the cyberlocker for user information, which is an expensive process and one that is not guaranteed to provide genuine contact details.⁷ Rights holders therefore are dependent on cyberlockers putting in place and enforcing repeat infringer policies, whereby users who are identified as having uploaded and distributed infringing files are barred from using the service. Although some cyberlockers claim to operate under such policies, there is little evidence of such policies being enforced.

- Challenges from URL, ISP, location, and equipment changes by such infringers: Because of the variety of names and sites, it is an easy matter for a systematic or repeat infringer to close down one site and open another. As noted above, it is difficult to secure accurate data from registrars. Unfortunately, many rogue sites do not even have to change their URL or ISP host in order to continue with their illicit operations. As stated above, domain name registrars generally are unwilling to enforce their terms and conditions regarding misuse of a domain name, which deprives rights holders of a simple and effective enforcement mechanism. In addition, although the majority of ISPs comply with their obligations under the DMCA and equivalent laws around the world (such as the E-Commerce Directive 2000/31/EC in the EU), several ISPs that are based outside of the U.S. refuse to comply with takedown notices, and thus become the hosts of choice for rogue sites.

Where sites are forced to change ISPs, it is all too easy to do so, often on a same-day basis, which causes minimal disruption to the site but requires rights owners to start from scratch with their takedown notice efforts. In one instance, the AAP, on behalf of a group of publishers, hired a law firm to take action against a site known as “Textbook Torrents” – although the site eventually came down, this was only after sustained pressure over several months during which the firm had to track the site as it changed ISPs spanning the U.S., the Netherlands, and finally, Canada.

⁶ There are two types of systematic infringers: those who upload content and those who download. Leaving aside “seeders,” this distinction is blurred in the context of the BitTorrent protocol as peer computers simultaneously upload and download, but it is valid in the case of cyberlockers, which as stated in these Comments provide the greatest level of anonymity to uploaders.

⁷ Identifying downloaders requires the same effort – unlike with the BitTorrent protocol where rights holders can in some instances observe and identify infringers based on the IP address of their computer, there is no way of independently observing whether and how often a file is downloaded.

Rights holder Experience with Key DMCA Provisions:

- ISP implementation of Sec. 512(i) (repeat infringer policy)

Due to U.S. case law defining this provision very narrowly to date, it has not been effective in requiring ISPs to adopt reasonable policies to prevent the re-listing of infringing content by pirates, or to prevent such identifiable or previously-identified infringers from listing other infringing content, forcing content owners to send takedown notices over and over again to address the conduct of the same infringers.

- Efforts to obtain injunctive relief pursuant to Sec.512(j)

To AAP's knowledge, thus far no publisher has relied upon the injunctive relief provisions of Section 512(j) provisions to seek injunctive relief against an ISP with respect to infringing material or activity on its system, so there are no experiences to report. Indeed, it is our understanding that there is no extant case law regarding the construction and application of Section 512(j), and that among the handful of court decisions that even mention those provisions, actions of the defendant ISPs – either in blocking access to the infringing material or activity, or in terminating a repeat infringing subscriber's access or account with the ISP – rendered the utility of seeking injunctive relief under its terms largely moot. But the chief inefficacy of seeking injunctive relief pursuant to Section 512(j) lies in its applicability only to ISPs that have been found both to be secondarily liable for infringement on their systems and protected from liability by one or more of the "safe harbor" provisions in Section 512. The costs and risk inherent in the implied requirement to bring an action against the ISP for inducement, contributory infringement, or vicarious liability provides a strong disincentive for attempting to utilize Section 512(j), and makes the provision virtually useless for purposes of pursuing legal action to address the posting of infringing materials or other online infringing activity when the ISP is foreign-based.

- Ideas to improve or add new legal remedies for more timely relief.
There is a significant need to incentivize the ISPs to monitor proactively for infringements and to use effective filters to detect and block, as well as to find and take down, infringing content before it proliferates.

Rightsholder Experience with Collaborative Approaches:

- Resulting replicable best practices, graduated response systems, etc.

AAP is encouraging file-sharing services to implement the attached set of "Principles and Best Practices for File-Sharing Websites and Services" written by our organization and its member publishers which we believe would significantly reduce piracy on the services if adopted. Measures include deploying technical filters to prevent infringing uploads of identified works, sending warning notices to infringing users of the services, terminating the accounts of users who repeatedly infringe despite the notices, and providing mechanisms for publishers to promote lawful versions of their products. The file-hosting sites Scribd.com and Wattpad.com have implemented filters which have been largely effective even if not 100% foolproof, and we are encouraging other services to do the same. Additionally, we believe that all file-sharing sites should post clear and conspicuous warnings prohibiting uploading infringing content, and that sites should communicate and implement robust policies against repeat infringers using their services.

Efforts to encourage ISPs to share information about repeat infringers also would be welcome, to the extent that implementing such a policy would be permissible under law. Further cooperation from domain name registrars regarding enforcement of their terms and conditions (specifically, terms that prohibit domain names that are registered through their services from being used for purposes that infringe third party rights) would also assist rights holders.

- Range of stakeholders participating in collaborations

Currently, most discussions appear to be limited to company or sector specific deals, where the individual companies enter into business relationships with the ISPs. Copyright owners should not be required to license content to sites in exchange for the site's agreement to adopt technological solutions that will reduce the amount of infringing content on the site. If the technology is available, the site should be required to use it.

- Best ways for government to encourage collaboration in private sector

The national governments of France, South Korea, and the U.K. have engaged in relatively successful initiatives with content companies, ISPs, and other interested parties to develop frameworks whereby repeat online infringers are discouraged from these activities by "graduated" enforcement steps, depending on how many times they have been warned about their infringing conduct and have nevertheless continued to engage in it. These efforts abroad prove that governments, content companies, and ISPs can indeed develop new solutions to meet the current challenges.

Where industry discussions without government involvement fail, government should consider how best to jumpstart and support these discussions.

Category 3: Internet Users – Consumers and User-Generated Content

Rightsholder Efforts To Address Internet Users:

- Efforts to improve User awareness of online infringement.

AAP applauds the role the U.S. Department of Education has taken to date to help institutions of higher education understand and implement the provisions of the Higher Education Reauthorization Act of 2008 mandating steps by colleges and universities to prevent the illegal downloading and distribution of intellectual property via their networks. AAP would welcome any additional steps by the U.S. government to educate the public about the importance of respecting copyright.

AAP has made a number of educational resources available on our Web site at http://publishers.org/main/AboutAAP/DivisionsCommittees/about_Comm_Roster_Online_Piracy.htm, including presentation slides, a list of examples of professionals who rely on copyright protection, a list of sources of legally-available digital versions of textbooks and other written works, and an audio recording of an NPR segment on the subject of textbook piracy online.

AAP and its members have also shared our Principles and Best Practices for File-Sharing Websites and Services document with the sites; the document encourages these services to take steps including, among other things:

- Use of technical filters to block infringing uploads;

- Sending of warning notices to the infringing users, notifying them that their actions violate copyright law and, furthermore, may result in termination of the person's use of the site;
- Maintenance and implementation of strict termination policies against repeat infringers;
- Posting of copyright protection policies in brief, plain language in conspicuous places on the site, and require users to sign click-through agreements to abide by these policies each time they seek to upload documents; and
- Providing publishers with access to titles-based reports on the number of blocked or removed infringements, as well as on the volume of warning notices sent to users.
- Efforts to improve availability and User awareness of legitimate sources for online access to copyrighted works.

Publishers routinely make e-book versions of their products available at the same time that the print versions are published, along with an ever-increasing number of backlist titles. More than 2 million legitimate e-book titles are already available for use on Barnes & Noble's Nook e-reading device⁸, and more than 750,000 books and other text-based products are sold on Amazon.com for use on the Kindle⁹. Other popular handheld devices on which a wide selection of e-book products can be read include Apple's iPad, Sony's line of e-readers, and many others. Through CourseSmart.com, publishers in the higher education market now offer low-cost electronic versions of more than 90% of the core textbooks currently in use in postsecondary instruction in North America.¹⁰

Rightsholder Experience with Miscellaneous Issues:

- Counter-notifications: appropriate and inappropriate use; volume

In our experience, there have been few issues regarding the inappropriate use of counter-notifications. Counter-notifications are very rarely sent in response to takedown demand notices from AAP member publishers.

- Reducing online infringement in foreign countries; on university campuses

In foreign countries:

Online piracy is inherently international in nature, due to the worldwide presence of sites and services hosting infringements. Furthermore, U.S. publishers' products are popular the world over. Improvements in the tools available to our industry and to the U.S. government to prevent online piracy of books and journals will be helpful toward combating infringement of U.S. publishers' products both domestically and abroad. As discussed on page 13 of these Comments, one of the sites which AAP and its members contended with in an international context in the past was TextbookTorrents.com, an indexing site which was facilitating and encouraging the posting and downloading of thousands of infringements of textbooks for the postsecondary education market. AAP

⁸ <http://www.barnesandnoble.com/u/nookcolor-feature-extras/379002479/?cids2Pid=35700>.

⁹ <http://www.amazon.com/Kindle- Amazons-Original-Wireless-generation/dp/B000F173MA>.

¹⁰ <http://www.coursesmart.com/overview>.

and a number of our member publishers hired the London-based law firm Covington & Burling to contact each ISP host used by the site's operator, who moved the site twice (from the U.S. to the Netherlands, and then to Canada) after the attorneys informed the first two hosts about the illegal nature of the site's activities. The site operator then voluntarily ceased his operations after the third ISP was contacted by the publishers' legal counsel.

On university campuses:

When monitoring of the public Internet by a publisher or its monitoring vendor indicates that a college or university appears to be the hosting ISP for a pirated file made available by a student or other individual on the campus, the publisher will send a takedown notice to the college or university in its capacity as the ISP. These notices are usually complied with by the institution. Furthermore, some of the antipiracy awareness materials made available by AAP at the link mentioned above

(http://publishers.org/main/AboutAAP/DivisionsCommittees/about_Comm_Roster_OnlinePiracy.htm) were written specifically to assist students and institutions of higher education (these include a list of legal sources of digital versions of textbooks and other instructional materials products; as well as a list of types of professionals who rely on copyright protection in their careers, to encourage students to take the issue of copyright protection into account as they consider their own potential career paths).

Exhibit A

Statement of Principles and Best Practices

Prepared by Members of the Association of American Publishers
February 2010

Introduction

This Statement of Principles and Best Practices is intended to address the growing problem of digital theft of content protected by copyright. The widespread infringement of copyright that occurs as a result of the dissemination of content without the copyright owner's authorization on websites, peer-to-peer file sharing services, blogs, bulletin boards, listing services and other services hurts everyone who is involved in the creation and legal dissemination of the content (such as raw materials providers and their employees, technology providers, sellers of advertising space, distribution and retail workers, shippers, and many, many more). Copyright gives creators the exclusive right to reproduce, create derivative works based upon, distribute copies of, publicly perform, and publicly display their works during the term of copyright. This incentive promotes creativity which benefits our culture, our economy, and our society.

All who use digital technologies should respect the exclusive rights held by copyright owners. Set forth below are Principles and Best Practices which we believe will support this goal.

Principles and Best Practices for File-Sharing Websites and Services

1. ENSURING THAT SITES ARE FOR LEGAL, NON-INFRINGEMENT PURPOSES

The site will take necessary steps to eliminate or seriously marginalize piracy, ensuring that their services are used predominantly for legal, non-infringing purposes. The site's business model shall not derive material benefits from piracy by users.

2. ADOPTION OF TECHNOLOGY SOLUTIONS TO REDUCE/ELIMINATE DIGITAL THEFT

The site shall not engage in direct copyright infringement or indirect copyright infringement – whether by knowingly inducing, contributing to or participating in infringement by another party or by failing to exercise the ability to control infringing conduct where the site directly benefits from the infringing conduct. Filtering Software is a technological measure that is widely available and should be used by all sites engaged in hosting, indexing, or disseminating content with the goal of eliminating from their services all infringing user-uploaded material. To that end, and to the extent they have not already done so, sites will fully implement commercially-reasonable Filtering Software that is highly effective, in relation to other technologies commercially available at the time of implementation, in achieving the goal of eliminating infringing content.

As of the date of this Statement of Principles and Best Practices, filtering systems are available using one or more of the following: keyword-matching applied to file names and file content; full and partial text matching applied to file content, combined with OCR (Optical Character Recognition) scanning of image-based PDF uploads to create texts of those files to check against the filter; and file-hash matching. To capture and store texts of publishers' books (such as by copying and storing files that have been the subject of takedown notices from copyright owners,

or OCRing image-only PDFs and storing the text), sites need to get the publisher's written permission on a company-by-company basis. Publishers may also provide reference data – such as keywords, titles, and partial or full text – for use in the filtering systems. Furthermore, sites will upgrade their systems as necessary to plug holes in the effectiveness of the Filtering Software that may be brought to the site's attention over time. The site will periodically (annually at a minimum) review, enhance and update the Filtering Software as new technology that makes a meaningful difference in achieving the goal becomes available. The site will also make available searching and identification technology to facilitate the ability of copyright owners to locate infringing content on all areas of the site.

When infringing content is removed by the site in response to a notice from a copyright owner, the site will notify the copyright owner of the removal, and permit the copyright owner to provide, or to request the site to provide on its behalf, reference data for such content to be used by the Filtering Software.

Sites which maintain a text-matching database for filtering shall work with the book publishing industry through the Association of American Publishers to identify agreed-upon technical security protocols to protect the database from unauthorized access and copying, and will also commit not to use or license the database for any purpose other than antipiracy filtering, nor to license or grant the database or its use to any third party without the written approval of all publishers whose works will be included.

3. CONSPICUOUS COPYRIGHT POLICIES

Sites will include in relevant and conspicuous places on their services information that promotes respect for copyright and informs users that they are prohibited from uploading and downloading infringing content. In plain language that is sufficiently brief to be read quickly and easily understood, sites shall prominently inform users during the upload process that they may not upload infringing content and that, by uploading content, they affirm that such uploading complies with the site's Terms of Use and copyright law. The Terms of Use shall prohibit infringing uploads.

4. MESSAGES TO USERS

In each instance where a user is found to have posted or attempted to post an infringement, the site will send a notice informing the user that her or his actions (or attempted actions) violate copyright law, exposing the person to legal liability as well as termination of the person's use of the site.

5. RESPONDING TO NOTICES OF INFRINGEMENT

- a. Sites should appoint a designated agent for receipt of notices of infringement and conspicuously post the contact information for the agent. In the United States, such appointment should be done pursuant to the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512.
- b. In the event that a site in the United States removes content pursuant to a notice of infringement, the site should comply with the requirements set forth in the DMCA as well as take the steps set forth below.

- c. In the event that a site (in or outside the U.S.) removes content in response to a notice of infringement, the site should (i) do so expeditiously, and (ii) in accordance with Section 4 above, notify the user who uploaded the content.

6. SPECIFIC POLICIES AGAINST REPEAT INFRINGERS AND TERMS OF USE

- a. Sites that follow the practices set forth in Sections 1 through 5 above should not have significant instances of repeat infringers. To the extent that repeat infringers exist despite the measures described above in this document, those individuals are likely to be engaging willfully in their repeated infringing conduct. The site will therefore implement policies containing stringent measures against repeat infringers, ultimately resulting in termination of the user's ability to upload content if the user persists in engaging in infringing activity.
- b. The site will use reasonable efforts to:
 - i. track infringing uploads of copyrighted content by the same user;
 - ii. implement a repeat infringer termination policy;
 - iii. prevent a terminated user from uploading copyrighted content following termination, such as by blocking re-use of verified email addresses and/or Internet Protocol addresses, as well as any associated payment account (such as PayPal); and
 - iv. remove all user content or other submitted content of repeat infringers.

At a minimum, the site will immediately terminate the accounts of users who

- On a maximum of three (3) separate occasions, have posted or attempted to post one or more files that infringe upon a publisher's work or works;
- In any individual instance have posted or attempted to post five (5) or more files that infringe publishers' works; or
- Have re-posted or attempted to re-post an infringement of a particular work after receiving a warning notice from the site in connection with the detection and takedown or blocking of the initial post.

7. RETENTION OF DATA

Consistent with applicable laws, including those directed to user privacy, the site will retain for at least 120 days: (a) information related to user uploads of content to their services, including Internet Protocol addresses and time and date information for uploaded content; and (b) user-uploaded content that has been on their services but has been subsequently removed following a notice of infringement. The site will provide that information and content to copyright owners as required by any valid process and permitted by applicable law.

8. REPORTING

Sites will, upon request and at reasonable intervals, provide publishers with title-based data on i) the volume of infringing uploads of publishers' works that have been found, attempted, blocked, and taken down; and ii) the numbers of warning notices sent as described in Section 4 of this document.

9. LINKING TO RETAIL PAGES

Sites and copyright owners should collaborate, to the extent technologically and commercially possible, to provide opportunities for sites to participate in publisher affiliate programs and for

copyright owners to market legal alternatives to purchase their content, including such alternatives as the placement of links to e-commerce web sites.

10. COMPLIANCE WITH APPLICABLE LAW

In engaging in the activities set forth in these Principles and Best Practices outside the United States, sites and copyright owners should follow these Principles and Best Practices to the extent that doing so would not contravene the law of the applicable foreign jurisdiction.

THESE PRINCIPLES AND BEST PRACTICES ARE NOT INTENDED TO BE, AND SHOULD NOT BE, CONSTRUED AS A WAIVER OF ANY OF THE RIGHTS OR REMEDIES OF SITES OR CONTENT OWNERS UNDER COPYRIGHT OR OTHER LAWS. THEY ARE NOT INTENDED TO, AND SHALL NOT, CREATE ANY LEGALLY-BINDING RIGHTS OR OBLIGATIONS ON THE PART OF ANY PARTY. SITES ARE SOLELY RESPONSIBLE FOR SEEKING APPROPRIATE LEGAL COUNSEL BEFORE IMPLEMENTING ANY OF THE MEASURES SET FORTH HEREIN TO ENSURE THAT THEY COMPLY WITH APPLICABLE LAWS.