BEFORE THE

OFFICE OF THE SECRETARY, U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE, U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION,
U.S. DEPARTMENT OF COMMERCE

Regarding:

Notice of Inquiry on "Copyright Policy, Creativity, and Innovation in the Internet Economy"
75 Fed. Reg. 61419 (Oct. 5, 2010)
[Docket No. 100910448–0448–01]

The American Association of Independent Music (A2IM); American Federation of Musicians of the United States and Canada (AFM); American Federation of Television and Radio Artists (AFTRA); Directors Guild of America (DGA); International Alliance of Theatrical and Stage Employees (IATSE); Motion Picture Association of America (MPAA); National Music Publishers' Association (NMPA); Recording Industry Association of America (RIAA); and Screen Actors Guild (SAG) (the "creative community organizations") appreciate this opportunity to respond to the above-referenced Notice of Inquiry (NOI).

The creative community organizations represent the companies and people who make and disseminate American motion pictures, television programs, music, and other copyrighted works. The livelihoods of millions of creators and workers depend on the continued growth and vitality of these creative industries. Brief descriptions of each of the creative community organizations can be found in Appendix I to this submission.

I. Introduction

Here are the main points the creative community organizations seek to convey in this submission:

1. The creative content industries are at the forefront in exploring and developing online business models for dissemination of creative works. But pervasive online copyright theft undermines these efforts. It also damages our economy, dampens innovation, and destroys American jobs that depend on creative activities. Beyond matters of dollars and livelihoods, the fundamental human rights of creators, as well as the health of our creative culture, are at stake.

2. This threat is not being effectively addressed today. A key missing element is widespread cooperation to combat online theft in the marketplace. The creative community is working hard both to build new business models and to engage in appropriate self-help measures. And some other players in the Internet ecosystem are working with us to support these efforts. Yet too many other players are not doing their part, because the current framework provides the wrong incentives. Even worse, others actively skirt the law, or even seek to undermine the cooperation that is needed.

3. To change this situation will take a combination of initiatives: continued industry innovation; greater inter-industry cooperation; government leadership; consumer education; expanded enforcement resources; continued litigation; and legislative changes. We must start now.

This filing sketches the current landscape, and the outlines of the needed responses. In Appendix II to this submission, we also provide answers to some of the specific questions posed in the NOI.

II. The Current Landscape

The creative community organizations are fully committed to providing creative works to consumers using the Internet. All the companies represented by our associations are actively building a wide variety of legitimate online outlets and alternative digital distribution forms, including electronic downloads of permanent copies of music, films and television programs; various rental and/or subscription businesses involving video or audio-on-demand and streaming; distribution over advertising supported streaming sites; and digital lockers for consumer storage and retrieval of purchased music, movie and television files.[1] Music, television and movie content is increasingly available to consumers when and where they want it, and using the device of their choice. This includes dissemination directly over broadband Internet connections via a wide array of devices, including personal computers, game consoles, Internet-connected televisions and Blu-ray players, smart phones, and stand-alone devices. All of these efforts and ventures have enabled millions of Americans to gain legitimate online access to music, film and television content in new and exciting ways. But all these efforts face a significant challenge: widespread online copyright theft.

A. Online copyright theft : a snapshot

What follows is a brief snapshot of the state of online theft of copyrighted materials as of December 2010.[2] We appreciate that the NOI's starting point is that "the prevalence of online

[1] For example, today there are more than 11 million legal tracks available online and nearly 400 legitimate services worldwide for the consumption of music, as compared to 1 million tracks and fewer than 50 services in 2003. *See* John Kennedy, IFPI, *Digital Music Report: Music How, When, Where You Want It – But Not without Addressing Piracy*, at 4 (2010) [hereinafter "IFPI Report"]. Today there are legitimate services through which a user can stream music to his phone, purchase the music on the fly, have music available "off the grid" for when the user is not connected to the internet, and listen to Pandora on his television, in his car or through his computer. This short list merely scratches the surface of the models being developed. In the audio-visual sphere, some of the new benefits to consumers include TV Everywhere authenticated online viewing; earlier on-demand windows that present an alternative to viewing movies in the theatre; more interactive offerings like BD-Live features in Blu-ray discs; licensed services like Yoostar that allow consumers to make mashups of their favorite content; and various industry innovations leading to legitimate cloud storage and interoperability of media files, such as UltraViolet and Keychest. A number of links to listings of legitimate online services are provided in the Appendix to this submission. *See* Discussion on Legitimate Ways to Exchange Non-Copyrighted Information on the Internet (Response 1K), Appendix II, at 4.

[2] This snapshot supplements the sketch of the online theft problem contained in the submission made by most of the creative community organizations last March, as input to the Joint Strategic Plan for Intellectual Property

(…continued)

copyright infringement" is a serious enough problem to provide the "primary motivation" for this proceeding. NOI at 64121. We also welcome the NOI's statements that this is "a persistent and significant problem," and that the resulting losses to "rights holders, the copyright industries, and the U.S. economy as a whole" are "substantial." *Id.* We also appreciate the NOI's quotation from the Joint Strategic Plan issued last June regarding the many ways in which online copyright theft harms our country. *Id.* However, to convey the scope and intensity of the threat, as well as its impact on the full range of affected parties, including consumers and Internet users as a whole, it is worth sharing a few striking analyses and examples. This is by no means a comprehensive survey of the problem, but simply a sampling of recent reports, most of them released within the past few months:

The Internet is awash with traffic in stolen intellectual property. Peer-to-peer (p2p) file sharing continues to account for at least 25% of all broadband traffic worldwide.[3] A very high proportion of this traffic involves unauthorized copies of movies, TV programming, sound recordings, and other copyrighted works.[4] BitTorrent and Gnutella, two p2p applications predominantly employed for unauthorized file sharing of copyrighted files,[5] rank first and third in the share of upstream North American traffic in peak periods for fixed access users, accounting for more than 45% of all such traffic; both also rank among the top ten for downstream uses.[6] A recent Princeton University study found that approximately 99% of 1,021 BitTorrent files reviewed violated copyright.[7] It is true that p2p's percentage share of total traffic is down from previous years; but in large part this is attributable to increased use of streaming services and cyberlockers as means for making stolen copyrighted materials available, as well as the rapid increase in mobile and other targeted applications dedicated to facilitating the theft of content. Research in the UK shows large increases in usage for unlicensed overseas MP3 sites, newsgroups, MP3 search engines, and forum blog and board links to cyberlockers, among other sources of pirate music.[8] McAfee estimates that the number of "live, active sites delivering illegitimate content" has sextupled since 2007, and notes "a growing number of

---

(…continued)
Enforcement. Letter from Creative Community Organizations to the Honorable Victoria A. Espinel, United States Intellectual Property Enforcement Coordinator (Mar. 24, 2010), *available at* http://www.mpaa.org/Resources/0c72c549-89ce-4815-9a71-de13b8e0a26f.PDF.

[3] Cisco Systems Visual Networking Index: Usage Study (Oct. 2010), *available at* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/Cisco_VNI_Usage_WP.html.

[4] Daniel Castro, Richard Bennett, and Scott Andes, The Information Technology & Innovation Foundation, *Steal These Policies: Strategies for Reducing Digital Piracy: Executive Summary* (December 2009), http://www.itif.org/files/2009-digital-piracy.pdf.

[5] *See* Ed Felten, *Census of Files Available via BitTorrent*, FREEDOM TO TINKER (Jan. 29, 2010), http://www.freedom-to-tinker.com/blog/felten/census-files-available-bittorrent. *See also* IFPI Report, *supra* note 1, at 21 (2010) (Seven million copies of Batman: Dark Knight were illegally downloaded using BitTorrent).

[6] Sandvine, *Fall 2010 Global Internet Phenomena Report*, at 15 (2010).

[7] Felten, *supra* note 5.

[8] *See* IFPI Report, *supra* note 1, at 19.

websites designed solely for attracting users and directing them to illegitimate sites."[9] And there is a disturbing acceleration in the number of mobile applications available that appear designed solely to search for and illegally download infringing music.[10] In a world of finite (even if growing) bandwidth, this massive flow of stolen copyrighted material reduces the space available for – as well as the competitive attractiveness of – legitimate services. This crowding out will be exacerbated as legitimate content distribution platforms move toward the HD content that consumers increasingly demand.

Online copyright theft continues to distort the legitimate market. In a recent week, the most popular film for download via BitTorrent – *Wall Street: Money Never Sleeps* – was still in initial theatrical release. So were three of the top 10 on the top downloads list.[11] These titles were being stolen in the first days of release, thus dramatically undercutting the downstream sales that will make the difference between profit and loss. Worse, some creative works illicitly appear online long before their release date.[12] *The Hurt Locker*, an independent film, won six Oscars, yet earned a surprisingly anemic $16 million at the North American box office, in significant part because unauthorized copies of the movie were "available on the Web months before its arrival in theaters."[13] The repercussions of this theft on the crucial downstream revenues for this film – on average, three-quarters of a film's revenue comes from markets subsequent to initial theatrical release, including online dissemination – are not yet known, but are sure to be damaging; the financial success of all independent films, and thus the ability to attract needed investment to finance future independent production, is jeopardized by online theft. The recent leak onto the Web of a track from Britney Spears' unreleased album[14] continues a disturbing and long-standing trend of online pre-release music piracy. Sometimes an entire album release must be aborted when tracks become available online, wiping out any chance that creators can capture value through authorized deals with legitimate media outlets.[15] In fact, in 2010 alone, virtually every Billboard top 500 album released by an RIAA member

[9] Paula Greve, McAfee, *Digital Music and Movies Report* (2010), *available at* http://newsroom.mcafee.com/images/10039/DMMRReport_US_25Aug2010.pdf, at 9 [hereinafter "Digital Music and Movies Report"].

[10] *See* Discussion on Patterns of Online Infringement (Response 1E), Appendix II, at 3.

[11] Eriq Gardner, *Piracy Hot List: "Wall Street," "Red," Britney Spears, CW's "Nikita"*, THE HOLLYWOOD REPORTER (Oct. 25, 2010).

[12] Despite significant, costly, and largely successful efforts that have been undertaken by all the major motion picture studios to secure their supply chain, including watermarking to curb internal leaks, some films still make their way onto the Internet prior to their legitimate theatrical release. Similarly, the music industry continues to work hard to develop and implement robust efforts to protect pre-release content from leaks, yet the problem persists.

[13] Richard Verrier, *Independent Filmmakers Feel the Squeeze of Piracy*, L.A. TIMES (Sept. 28, 2010).

[14] *See* Gardner, *supra* note 11.

[15] The Spanish experience may offer a cautionary tale for larger markets, including the U.S. In a market with one of Europe's highest usage rates of illicit p2p services, the legitimate music market has shrunk to 1/3 of its 2001 size. Significantly, local acts were hard hit: their share of sales in Top 50 dropped by 65% from 2004-09. *See* IFPI Report, *supra* note 1, at 19.

either had a prerelease track leaked prior to the album's debut, or was subject to an attack attempting to leak a pre-release track. Needless to say, this causes a lot of disruption and is incredibly damaging.

Online theft hurts independent creators as much as, and more immediately than, major studios or labels. Consider the situation of Ellen Seidler, an independent filmmaker who refinanced her home and maxed out her credit cards to produce *And Then Came Lola*, which turned up online without authorization within 24 hours of its DVD release. In the next five months, Seidler "found close to 20,000 links to pirated copies of her film."[16] Another independent filmmaker, Greg Carter, who "spent the last three years scraping together $250,000 to write, direct and produce *A Gangland Love Story*, lost an estimated $100,000 in revenue after his work, available for unauthorized free download from sites in six countries or via links from 60 different websites, was viewed online 60,000 times in the first two months after its release, "dashing hope that he'll ever see a profit."[17]

The impact of online theft is felt throughout the workforce. Film and television performers, directors and assistant directors, songwriters, recording artists, background musicians and vocalists, and the many craftspeople on (and behind the scenes of) film shoots, TV productions and recording sessions are all affected by online theft. The loss of downstream revenue in the form of residuals and royalties has a very direct impact on the livelihoods of all who are part of the creative process that is filmmaking and sound recordings. The importance of downstream revenue is not to be ignored; for instance, on the audiovisual side, 75% of a motion picture's revenue comes from markets after the initial theatrical release, and more than 50% of scripted television revenues are generated after the first run. In 2009, AFTRA recording artists derived 90% of their recording-related income from physical CD sales and paid digital downloads, two distribution channels most undermined by online theft. DGA, IATSE and SAG members rely heavily on residuals and royalties from "downstream" uses of films and TV programming – everything after initial broadcast on television or exhibition in a theater – not only for direct compensation (in 2009 DGA members derived 19% of their compensation from residual payments and SAG members who work under the feature film and television contract derived 45% of their compensation from residuals), but also for funding health and pension benefits; for instance 65% of the health plan for IATSE members, and 71% of DGA's basic pension plan, are funded by revenues from TV broadcast of films, and "supplemental markets" (e.g., DVD, Pay TV, etc.) for film and TV programming.[18] Session musicians in both the recording and film industries depend for significant portions of their income on AFM-negotiated funds that share with musicians the proceeds of legitimate sales (including online) of recordings and music videos, and of supplemental market uses of films. All these markets (including new media) are undermined when the works are available for free download or streaming without authorization.

---

[16] Greg Sandoval, *Indie Filmmakers – Piracy and Google Threaten Us*, CNET (Sept. 20, 2010).

[17] *See* Verrier, *supra* note 13.

[18] Am. Federation of Television and Radio Artists, et al., *Online Theft: The Impact on Film Television, and Music Industry Creators, Performers, and Craftspeople* (Aug. 2010) ("Online Theft Fact Sheet"), attached as Appendix III.

Consumers, too, are damaged by online theft. A recent McAfee "Digital Music and Movies Report" documents "the true cost of free entertainment," noting that "sites that are set up to distribute illegal content ….often distribute malware and expose users to other risks…. The sheer demand for streaming content makes it very appealing to cybercriminals," and many pirate sites have "criminal associations." The McAfee report concludes that "cybercrime is big business, and online media is one of cybercriminals' biggest moneymakers."[19]

Online theft has been linked to organized crime and to terrorist financing. In a statement to the House Committee on Foreign Affairs on July 21, 2010, U.S. Immigration and Customs Enforcement Assistant Secretary John Morton testified about a recent anti-piracy operation that tied a U.S. based stolen property and counterfeit goods syndicate in Philadelphia, whose inventory included pirated DVDs, to Hezbollah, and which used the proceeds of the sales to procure weapons. The operation led to 25 indictments, and 15 criminal arrests.[20] Additionally, a March 2009 study from the RAND Corporation concluded that film piracy by organized crime worldwide is flourishing, supplementing crime syndicates activities related to drugs, money laundering, and human smuggling.[21]

These snapshots underscore the seriousness of the challenge that online copyright theft poses to our economy, our society and our culture. The question for this NOI is whether our policy and enforcement tools are sufficient to meet that challenge, and if not, how they should be improved.

B. The legal and policy landscape

While it is not the only relevant provision of the copyright law with regard to the fight against online copyright theft, much discussion has focused on the Digital Millennium Copyright Act (DMCA), and specifically on 17 U.S.C. § 512, the Online Copyright Infringement Liability Limitation Act, enacted in 1998 as title II of the DMCA. Congress enacted this provision of the DMCA primarily to "preserve strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[22] Congress also responded to a demand from service providers for "greater certainty … concerning their legal exposure for infringements that may occur in the course of their activities."[23] A dozen years of experience under this statute demonstrate that while service providers may have enjoyed their end of this bargain – their legal exposure is more certain – copyright owners have not – the incentives for cooperation have fallen short. Consequently, Congress's primary objective has not been achieved.

---

[19] Digital Music and Movies Report, *supra* note 9, at 4, 14.

[20] *See Protecting U.S. Intellectual Property Overseas: The Joint Strategic Plan and Beyond, Hearing Before the House Committee on Foreign Affairs*, 111th Cong. (July 21, 2010) (statement of ICE Assistant Secretary John Morton), *available at* http://foreignaffairs.house.gov/111/57607.pdf.

[21] *See generally* GREGORY F. TREVERTON, ET AL., FILM PIRACY, ORGANIZED CRIME, AND TERRORISM (Rand Corp. 2009).

[22] S. REP. NO. 105-190, at 40 (1998).

[23] *Id.*

The DMCA was an effort to provide a balanced and effective set of incentives for the creative, technology and telecommunications communities to work together to "detect and deal with" online copyright theft. For a variety of reasons, the DMCA has not lived up to that promise. Unfortunately, as applied by some courts and as interpreted by many service providers, the safe harbor provisions of the DMCA provide misplaced incentives that fail to promote meaningful cooperation, resulting in too many cases in indifference, or willful blindness to the widespread infringement that takes place on their systems or services. Cooperation sometimes occurs, and we welcome and encourage it. But the incentives to cooperate are too weak, and as a result, cooperative efforts often fall far short of an effective response to the destructive phenomenon of online theft.

A great part of the problem is the misperception of the DMCA as nothing more than a "notice and takedown" statute. Too many industry players, policymakers, and even some federal courts believe that, if a service provider responds to notices received from the copyright owner regarding specific individual instances of copyright infringement that the copyright owner has been able to detect, then the provider escapes all responsibility for infringement occurring on its service, even if the provider has encouraged the infringement, either explicitly or through the design of its system. Indeed, the wording of this NOI contributes to this misperception by stating that the DMCA "safe harbor is predicated on a 'notice and takedown' regime." NOI at 61423. In fact, however, the DMCA is not just about notice and takedown. The law imposes important conditions on any safe harbor, conditions that extend well beyond participating in "notice and takedown." The neglect of these other conditions is the leading reason why the promise of the DMCA – to encourage inter-industry cooperation against copyright theft – has not been fully realized.

Some erroneous lower court decisions have contributed significantly to this trend. In several cases arising under section 512, lower federal courts have:

- Applied safe harbors to activities well beyond their statutory scope. Particularly in the case of the section 512(c) safe harbor, which applies to infringement claims "by reason of storage [of content] at the direction of a user," some lower courts have held that entire on-line businesses that are founded on online dissemination of copyrighted material fall fully within the safe harbor because their functions also involve storage.[24] Such a reading redirects a statute that was aimed mainly at sheltering businesses from liability for infringements that occur inadvertently or unavoidably, in the course of providing specific online functions. It risks distorting the DMCA into a law to provide substantial "breathing room" for online businesses founded almost entirely on the unauthorized dissemination and exploitation of creative works.

- Given short shrift to other requirements that service providers act in order to claim the safe harbor. Under section 512(c), for example, service providers must remove infringing materials or activities from their networks if they have "actual knowledge" of infringement, or if they become "aware of facts or circumstances from which infringing activity is apparent," even if that knowledge or awareness does not arise from receiving a

[24] *See, e.g.*, Viacom v. YouTube, 540 F. Supp. 2d 461 (S.D.N.Y. 2008).

notice from a right holder that meets the technical requisites of the statute. Some court decisions have read these "actual knowledge" and "red flag" tests very narrowly, giving service providers an excuse to do nothing to combat pervasive and even blatant infringement, unless and until they receive a compliant notice about a specific infringement. *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007) (finding that website names such as "illegal.net" and "stolencelebritypics.com" were not "red flags" because "describing photographs as 'illegal' or 'stolen' may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen"). This invitation to inaction runs counter to the design of the law, which sought to stimulate active cooperation, not passivity, in "detecting and dealing with" online infringement.

- Made it extremely difficult even to give effective notice in the mass piracy environment. The practical reality is that large repertoires of creative works need to be safeguarded against high-volume and high-velocity infringement. Conceiving the system as limited to specific notices for specific works dooms it to failure and effectively eliminates the needed protection. Treating the DMCA as part of "an area of law devoted to protection of distinctive individual works, not of libraries" betrays a naïveté about 21st century commercial realities. Viacom International, Inc., v. YouTube Inc., at *29 (S.D.N.Y. 2010).

- Devalued the "repeat infringer" requirement. The DMCA made the implementation of a reasonable "repeat infringer policy"– providing for the termination "in appropriate circumstances" of the accounts of subscribers or account holders (both individual and commercial) who repeatedly infringe copyright – the sine qua non of every safe harbor for every category of service provider, even the "mere conduits." 17 USC § 512(i)(1)(A). Clearly this obligation was meant to apply whether or not the service provider learned of these infringements through notices from right holders or otherwise. But a widely followed line of court decisions has reduced this requirement to a mere appendage of the policy of responding to takedown notices. These courts have held that, for purposes of this requirement, "a service provider 'implements' a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications." *CC Bill*, 488 F.3d at 1107 (9th Cir. 2007). Under this very relaxed standard, the presence of defects in notices sent to the service provider appears to allow the provider to ignore all such notices for purposes of its repeat infringer policy, *id.* at 1112, as well as to overlook other evidence it may have regarding repeat infringement. The independent obligation to deal with repeat infringers without regard to DMCA takedown notices has virtually vanished from the perspective of these courts.

Statutory notice and takedown remains important, and one policy goal should be to reinvigorate its effectiveness as part of the response to online copyright theft. But a bigger problem has emerged in the dozen years since enactment of the DMCA: more and more of the online theft problem has migrated to other technologies that fall outside the notice and takedown framework, or even outside the rest of Section 512. To this degree, the problem is not just the "tunnel vision" of some courts or commentators, or the fact that too many service providers do no more than the bare minimum. It is that the DMCA, while perhaps well suited to the online

environment of 1998, did not adequately anticipate the online theft challenges of the 21st century, and as a result does not comprehensively addresses the online theft problem it was designed to combat. For example:

1. A large proportion of online infringement takes place through the use of decentralized p2p applications such as BitTorrent. These applications are extremely complex and involve distinct entities –peers, trackers, torrent-indexing sites – with distinct functions. It is clear, though, that "material stored by a service provider at the request of a user" – the paradigm for the section 512(c) notice and takedown process – plays a minimal role in the way that stolen files are propagated and distributed in the BitTorrent environment. Even the role of the torrent-indexing sites is far different from what Congress was confronted with when it enacted section 512(d), dealing with "information location tools." Any effective strategy for dealing with dissemination of infringing material via BitTorrent or similar means requires cooperation from "mere conduit" service providers, to identify and educate users engaged in such conduct. But the DMCA obligations of such providers are even lighter than for other entities, and too often the needed cooperation is lacking.

2. Much of the most blatant copyright theft has moved offshore, to sites not directly subject to the DMCA (and thus often not even amenable to notice and takedown). Of course these sites are often dependent upon US-based companies to provide revenue (through advertising and/or financial transaction services), and even for bringing US customers to their stolen-property bazaars (whether through ISP access or via search engines). The tools provided under current law for cracking down on these sites and for cutting off their means of support may not be sufficient.

3. A growing share of the problem involves scenarios in which time is of the essence, such as unauthorized real-time streaming of telecasts; sites that shift rapidly among different hosts and ISPs, both within and outside the US; and the rapid proliferation of mobile applications dedicated to facilitating infringement. The DMCA model, especially notice and takedown, can be too slow and cumbersome to respond effectively in these circumstances. In some cases of streaming, for example a live concert or sports event, a delay of just one hour in responding to a takedown request can render the notice-and-takedown process wholly ineffective. Copyright owners increasingly need to be able to rely on the cooperative efforts of sites that facilitate such conduct to block or remove infringing retransmissions in real-time. Sites that provide a constantly refreshed index of links to infringing content, or that disseminate mobile applications dedicated to infringement, also propagate very quickly, and demand a comparably rapid response.

C. Result: the law rewards inaction rather than cooperation

A wide spectrum of legitimate online services seek to reap the full benefits of a safe harbor simply by responding in some manner to DMCA-compliant notices, while maintaining "plausible deniability" of widespread theft that abuse of their services enables or facilitates. While some such services are more forward-leaning in addressing online theft, too many others fail to take commercially reasonable steps to reduce theft levels, even when they are clearly able to do so without penalizing legitimate customers. The balanced approach intended under the DMCA has been lost; and meanwhile, the challenge of online copyright theft has mutated into

forms for which the current law is not as well adapted. The misapplication of DMCA immunity for service providers leads, as a practical matter, to impunity for some of the most serious infringers.

III. Solutions: Issues that must be addressed

Responsive to the NOI's stated goals, we offer the following non-exhaustive menu of issues that should be addressed as part of a policy framework that will "combat online copyright infringement more effectively" while "sustain[ing] innovative uses of information and information technology." NOI at 61420. In many instances, these involve steps to vindicate Congress's intent in enacting the DMCA, by revitalizing the best practices Congress set out in that statute for entities claiming liability safe harbors.

A. Repeat infringer policies were intended to be the gateway to any safe harbor against infringement liability – whether or not notice and takedown was applicable. The main goals of such policies are persuasive, not punitive: they can be powerful tools for educating website operators about the dangers and the full costs of disseminating stolen copyrighted materials online and for educating consumers about the dangers and the full costs of acquiring such materials, and an efficient means of encouraging change to more responsible behaviors. But, as noted above, the courts have been lax in enforcing this requirement. While some intermediaries, such as some ISPs and hosting services, respect this obligation, to our knowledge, too few of them implement such policies in a way that has any educational value – or real consequences – for website operators or consumers. The issue is not simply about termination of service, but about the refusal in some cases to forward notices containing the details about the infringement; to escalate subsequent notices to ensure they are read and understood; or even to employ lesser forms of meaningful deterrent measures that could change behavior on a broad scale.

To a great extent, this part of the solution to the problem is solely in the hands of service providers. At least as to consumers, because an individual account holder's connections to the Internet may change with each session or on some other periodic basis, right holders often have no way of knowing who are the repeat infringers, while this information is readily accessible to the providers. We know that all significant service providers state that they oppose copyright infringement, and their terms of service with customers almost always forbid use of their services for that purpose. But as far as the creative community organizations have been able to observe, only a handful of service providers take steps to make these statements of intent a reality, in a way that has the capability to change customer behavior. If the facts are otherwise, we urge service providers to present them in this proceeding.

The experience of one category of service providers that has, in a number of instances, actually implemented repeat infringer policies may be instructive. Spurred in great part by enactment of Higher Education Opportunity Act (HEOA) provisions on this topic, many higher education institutions have taken steps to deal with the problem of widespread copyright infringements on their own networks. The HEOA required schools to alert students to the law; to plan to "effectively combat" infringement on the network, including through "the use of one

or more technology-based deterrents;" and to offer or suggest legal downloading alternatives.[25] Even before the HEOA, however, universities were implementing policies and practices to address the problem. These ranged from simple educational campaigns to the use of commercial products to limit p2p use.

While universities have varied widely in their practices, it is striking how many have chosen on their own to implement a tiered response system. Students caught engaging in online copyright theft frequently risk fines, referral to disciplinary authorities, disruption and termination of access, and in some cases suspension or even expulsion from school. For example, Vassar imposes twenty hours of community service upon an initial violation, which doubles upon subsequent violations.[26] Central Washington University begins by disabling users' access for one week, escalating to two weeks, and finally indefinitely upon a third violation.[27] The University of Delaware imposes a $75 fee upon the first violation, escalating to $110 upon a second, and network access is disabled until the student completes a copyright education course and examination of the computer by IT officials.[28] An escalating re-connection fee is imposed at Stanford University.[29]

The university experience has been that the most severe penalties do not need to be imposed very often. As Kip Cox in the Office of the Dean of Students at the University of Wisconsin stated: "Very few students get a second offense…. The ones that are aware of it usually stop after the first time."[30] Dennis Gendron, Vice President for communication and information technology at Middle Tennessee State University, noted that, "[Violating] students were identified, disusered, counseled, and returned to polite society without a repeat offense."[31] From receiving fewer infringement notices to reclaiming valuable bandwidth, such decline in infringing behavior on p2p networks, due merely to the threat of increased penalty, has worked extremely well for schools.

A credible threat of meaningful sanctions against repeat infringers on non-campus networks would send a powerful message. It would not take many such instances to significantly change both commercial and individual subscriber behavior and deter millions of other consumers, and new website operators, from engaging in copyright theft. Of course, the need for

---

[25] Higher Education Opportunity Act, Pub. L. 110-315, 122 Stat. 3078 (Aug. 14, 2008).

[26] John W. Barry, *College Students Face Penalties for Sharing Music Files*, , POUGHKEEPSIE JOURNAL (June 29, 2010).

[27] Central Washington University, Information Technology Services Department: *Acceptable Use Policy*, http://www.cwu.edu/~its/acceptable-use-resnet.pdf.

[28] University of Delaware, Computer Security: *The Bottom Line on File Sharing at the University of Delaware*, http://www.udel.edu/security/cr_response.html.

[29] Stanford University Libraries and Academic Information Resources webpage, Information & News: *File-Sharing and Copyright Law: How it Affects You*, http://rescomp.stanford.edu/info/dmca/.

[30] Jennifer Zettel, *File Sharing to Get Trickier*, THE BADGER HERALD (July 20, 2010).

[31] Heidi Hall, *Universities Face Punishment for Allowing Illegal File-Sharing*, NASHVILLE TENNESSEAN (July 2, 2010).

strong and well-implemented repeat infringer policies is by no means confined to end-users on a digital network. It must also apply, for example, to bloggers or renters of online lockers who repeatedly use these mechanisms to make infringing content available, and to site operators whose content is hosted by hosting service providers and access to which is facilitated by access service providers.

B. Use of technology to advance cooperative efforts. Right holders must have the ability to search for infringement online, and to send notices, that is commensurate with the scope of infringing activity that they must combat. It is striking that technologies for achieving this goal have taken a quantum leap since 1998. The technological means for automated identification of copyrighted materials are much more readily available in the marketplace, far more scalable, and much more effective than they were when the DMCA was enacted.[32] Furthermore, right holders increasingly apply robust, standards-based monitoring and verification techniques to their enforcement activities, so that service providers and consumers can be confident that the findings are valid, and so that legitimate personal privacy interests are respected.[33] Yet many service providers rely upon the mantra that they have no responsibility to monitor how their services are used, and even impede access for right holders seeking to monitor these services for themselves. For example, Google has available an application program interface that would help automate search results for infringing content on the Google search product. Press reports had previously noted that Google planned to charge rights holders up to several million dollars to use the same API.[34] And other similar service providers have been hesitant to provide to rights holders access to similar APIs at all. Even though highly effective automated systems for matching online content to copyright reference databases are readily available, and are currently in use by some service providers,[35] other providers feel no obligation to implement them, or even to discuss doing so. Even though another provision of federal law could give service providers broad immunity from liability for employing such technologies to filter their customers' access to "objectionable materials," uptake is hampered by the lack of any meaningful incentives to do so.[36]

---

[32] Although the DMCA has a provision requiring accommodation of standard technical measures, 17 U.S.C. § 512(i)(1)(B), it has proven to be a dead letter over the past dozen years, perhaps because it is so narrowly drawn.

[33] *See* Discussion of Internet Intermediaries: Safe Harbors and Responsibilities (Response 2B), Appendix II, at 4-5.

[34] Greg Sandoval, *Big Media Wants More Piracy Busting from Google*, CNET (Oct. 13, 2010), http://news.cnet.com/8301-31001_3-20019411-261.html. More recent reports indicate that Google has retreated from these plans, and we welcome that development. *See* Blog Post by Kent Walker, General Counsel, Google, *Making Copyright Work Better Online* (Dec. 2, 2010), http://googlepublicpolicy.blogspot.com/2010/12/making-copyright-work-better-online.html.

[35] For example, signatories to the UGC Principles, such as MySpace, DailyMotion, and Soapbox, etc., employ the Vobile content recognition/filtering system. Note also the Content ID system used by YouTube.

[36] 47 U.S.C. § 230(b) provides: " No provider … of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider … considers to be …. otherwise objectionable, whether or not such material is constitutionally protected". Of course, many providers already protect themselves contractually against any claim from a customer arising from removal of access to infringing material, but the provision just quoted is broader and has been applied in the case of filtering of

(…continued)

There are some exceptions. For example, leading UGC sites presently use filtering technology so that infringing content is not made widely available on the Internet in the first place. But for the rest, at the very minimum, these entities must take reasonable steps to enable the creative community to help itself in combating this threat. In the current enforcement environment, copyright owners already bear the initial burden of monitoring the online environment for instances of infringement. This framework is undermined when service providers limit the functionality of automated crawlers or similar reasonable and lawful technological means for identifying infringements, or when they deny copyright owners or their agents reasonable access to the provider-controlled online venues where infringement occurs.

C. Notice and takedown reform. Although, as noted above, this technique is not as effective against some of the most significant forms of online copyright theft, it remains important, and it must be adapted to the current reality: an environment of high-volume and high-velocity online infringement. From the earliest days after enactment of the DMCA, both the generation of takedown notices and the response to them by online service providers have been automated to a considerable extent. The case could hardly be otherwise, considering the scope of infringement and the nature of the services where infringement is taking place. Right holders need to protect entire repertoires, not just individual works. Law and policy should recognize this reality, and not pretend that the norm is for individual notices about individual works to be individually prepared and sent, and individually evaluated upon receipt. Although the statute provides that a compliant notice need not name every work infringed if a "representative list" is provided,[37] service providers often fail to respond to such lists, and too often the lower courts have declined to meaningfully enforce it.

In order to revitalize notice and takedown, copyright owners who own or manage large portfolios of works should be able to make available for service providers' reference an authoritative and readily usable database of works or digital files; and service providers should be expected not only to take these files down, when they are identified online directly or when the service provider receives a takedown notice about one of them, but also to employ reasonable efforts to keep them down, by prohibiting the uploading or linking to infringing content previously subject to a takedown notice. The "takedown" part of the equation should also be viewed as including an obligation to take commercially reasonable steps to "keep down" an item once it has been removed, and not allow it to be re-posted by the same or a different user (or thousands of such users) on the same or other services operated by the same provider. This would be especially valuable to smaller copyright owners and individual creators who lack the resources for the intensive and unremitting monitoring that the current system demands. Commercially available detection technologies, which have advanced considerably since enactment of the DMCA, can readily facilitate implementation of a "keep down" policy. Service providers should not find their claims to safe harbor status in jeopardy when they agree

(…continued)
material available to users of digital networks. *See, e.g.*, Zango v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009).

[37] 17 USC § 512(c)(3)(A)(ii).

to monitor and block infringing content in this way; to the contrary, such cooperation should be encouraged as anticipated by Congress in enacting the safe harbor.[38]

The statutory requirement[39] that takedowns occur "expeditiously" must also be revitalized, in light of the disturbingly common practice of some search engines to review all takedown requests for up to multiple weeks.[40] In this regard, we note the constructive December 2 announcement by Google – whose takedown policies have been widely criticized for excessive delay – that "over the next several months," it will change its practices and act on "reliable copyright takedown requests within 24 hours."[41]

D. Enhanced cooperation against online thieves. Especially for the online sites most egregiously dedicated to theft, a mechanism is needed to expeditiously cut thieves off from the services they need to survive: payment processing, advertising placements, web hosting, search engines, and customer access via ISP. Some payment processing and other services have stepped up to cooperate with right holders to rid their own customer and subscriber lists of online thieves, including through comprehensive "repeat infringer" policies. But more must be done to encourage such voluntary cooperation; and the current very limited availability of injunctive relief against such intermediaries falls short as well.

E. Problems beyond theft.

While online copyright theft is certainly the major obstacle to a thriving legitimate online marketplace in copyright works, it is not the only one. Surely legitimate services face an formidable challenge to compete against criminals, who not only do not need to recoup the often enormous costs of creating a copyrighted work, but who also pay no royalties, no taxes, and incur no costs for regulatory compliance. Even in the face of this widespread theft, creators and copyright owners have been aggressive and creative in pursuing new business models for online distribution. But these new models will struggle to take hold so long as the creative sector is undermined by pervasive online theft in the meantime.

---

[38] DMCA Conference Report, H.R. 2281, H. Rept. 105-796, at 73: "This legislation is not intended to discourage the service provider from monitoring its service for infringing material. Courts should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program."

[39] 17 USC § 512(c)(1)(C).

[40] *See* Discussion of Tardy Takedowns (Response 2E), Appendix II, at 7.

[41] *See* Blog Post by Kent Walker, General Counsel, Google, *Making Copyright Work Better Online* (Dec. 2, 2010), http://googlepublicpolicy.blogspot.com/2010/12/making-copyright-work-better-online.html. Google's announcement outlined a number of other potentially constructive steps for more effective enforcement against copyright infringement taking place on its services. The creative community organizations welcome this initiative as an indicator that Google recognizes the importance of shared responsibility for addressing these serious problems, and will be following closely to see if the new policies are implemented in a way that will help them achieve this potential. However, we also note that a handful of service providers already provide takedowns that are nearly instantaneous, and that in several contexts, such as when movies are in theatrical release or with respect to prelease music, delays of 24 hours are too long.

Beyond the challenge to compete with thieves, we face other roadblocks, which are discouraging investment in, and needlessly driving up costs of, online delivery models. Government could play a role in removing these, by:

1. Ensuring that federal policy is helping – not hindering – in the development of game-changing business models for access and consumption of content, particularly music. For example, for a music service to be successful, it must offer consumers far more content than just the music of one or two companies. Yet game-changing music business models raise numerous challenging issues that need to be addressed, and it is difficult to gain consensus on how to handle such issues (like DRM, tethering, sharing among computers, royalty distribution methodologies, allocation of royalties among classes of right holders, and many more). For truly innovative services to be launched, federal policy should permit limited collaboration among licensors and licensees to help develop and define these business models.

2. Fashioning any communications law rules for network access to serve the twin goals of minimizing interference with legitimate proactive technologies and practices aimed at combating online copyright theft, while protecting the free flow of lawful goods and services.

IV. Solutions: How to Get There

Four aspects of the path forward deserve mention here.

A. Voluntary agreements/best practices

For a number of reasons, this is clearly the best option for making progress in the fight against online copyright theft. When the industry players directly involved in the online marketplace come to the table, they bring unmatched expertise and real world experience. They can be well positioned to craft an agreement, and/or a set of best practices, that is both realistic and flexible, and that takes directly into account the costs of compliance or implementation. The parties can also reconvene quickly in order to adapt their agreement to take account of significant changes in the marketplace or advances in technology, either on the side of the infringers or on the side of those seeking to enforce their rights. A regime imposed on the parties by the government would be far less desirable, and likely far less effective, in all these aspects.

But for this strategy to work, the parties must come to the table and be prepared to cooperate. We are encouraged that some leading Internet Service Providers and other intermediaries have taken a constructive approach, reflecting their commitment to good corporate citizenship. They appear to understand that the Internet is less likely to thrive in the long run if theft and illegal activity continue to play such a prominent role in the marketplace in which they operate, and that the healthy development of a legitimate e-commerce marketplace in copyrighted materials will benefit everyone. Unfortunately, too many of their counterparts do not yet see things this way. Some significant parties in the Internet ecosystem seem to lack a good reason to come to the table.

For these reasons, meaningful voluntary agreements in this field have been rare. The Principles for User-Generated Content cited in the NOI is a positive example of how right holders and service providers can come together "to protect copyrighted works and to bring more

content to consumers through legitimate channels." NOI at 61423. University action and collaboration with rights holders, examples of which can be seen on EDUCAUSE's "role models" website, is another case in point.[42] As noted above, some ISPs and other intermediaries have engaged in constructive discussions about cooperative efforts. The creative community organizations commend these responsible companies and institutions. But there are very few other examples to point to. The legal environment we face today is a major contributor to this shortfall, because too many intermediaries see it as a basis for passivity and willful blindness.

Strong federal leadership could make a difference. The government is in a good position to communicate to all parties that the purpose of granting immunity to intermediaries was not to encourage them to turn a blind eye to the rampant theft that all can see. As the NOI notes, the Joint Strategic Plan on Intellectual Property Enforcement encourages voluntary cooperative efforts. *Id.* The creative community organizations strongly support this aspect of the Joint Strategic Plan, and will work with the U.S. Intellectual Property Enforcement Coordinator to advance these critical first steps by the government to encourage all parties to come to the table. Best practices developed by a range of the interested parties could help to quell competitive concerns that might otherwise, for example, discourage adoption of a more vigorous repeat infringer policy.

Unfortunately, not everyone who might seek a place at the table is positioned to make a constructive contribution. The creative community organizations have been dismayed to see some groups allow themselves to become professional apologists for online theft. Such groups seem to reflexively label every step taken by copyright owners against online theft as a mortal threat to the Internet;[43] continually predict dire outcomes if the arguments of copyright owners and creators prevail;[44] support enforcement strategies in the abstract, only to attack them as soon

[42] http://www.educause.edu/HEOArolemodels.

[43] *See, e.g.*, AFP, *P2P Case Comes Up This Week*, THE AGE (Mar. 28, 2005) ("Allowing entertainment companies to sue technology innovators for every infringement will chill innovation and retard the entire sector . . . . [T]he Betamax decision has been with us for 21 years, and the technology and entertainment industries have flourished in that time. We see no reason to turn back now.") (*quoting* Fred von Lohmann, Electronic Frontier Foundation); Computer & Communications Industry Ass'n, et al., Amicus Brief in support of Respondents, MGM v. Grokster, 545 U.S. 913 (2005) ("If petitioners' theories are adopted, virtually all digital technologies will be subject both to advance clearance by a small group of content conglomerates and to after-the-fact second guessing by virtually any copyright owner about how the technology was designed and how it is being used. If a technology provider guesses wrong, it will be subject to potentially ruinous statutory damages. Innovation and investment cannot survive in such an environment."); Grant Gross, *Grokster Case May Have Large Impact Beyond P-to-P*, COMPUTERWORLD (Mar. 25, 2005) ("Demanding that innovators guess how people use a new technology, and holding them liable retroactively if they fail to anticipate what users will do . . . is a radical new definition of secondary liability that will chill innovation . . . The tyranny of copyright risk and the liability it will bring will make innovators timid in inventing new communications technologies.") (*quoting* Mark Cooper, Consumer Federation of America).

[44] *See, e.g.*, Gary Shapiro, CEA, *MGM v. Grokster: Notable Quotes*, ONLINE REPORTER (Apr. 2, 2005) ("[If the courts rule in favor of the copyright owners] we may witness the end of popular and revolutionary products and technologies such as the iPod, TiVo and even the Internet itself, and also the premature deaths of thousands of products that only exist as a concept in the minds of young entrepreneurs."); Charles Lane, *High Court to Weigh File Sharing*, WASHINGTON POST (Dec. 11, 2004) ("The evidence that file sharing has significantly hurt the large content companies is very thin. But the tradeoff of giving content companies more control over the development of technologies and of overturning Betamax would be very significant and very harmful to consumers and to our economy."); Ben Fritz and William Triplett, *High Noon for Digital Players*, DAILY VARIETY (Mar. 28, 2005) ("If

(…continued)

as they are deployed;[45] stoutly defend technologies that are widely used to steal copyrighted materials, while attacking technologies that could be used to defend copyright;[46] predictably oppose virtually all proposals for better or more efficient copyright law enforcement;[47] and sometimes even encourage intermediaries to follow a path of "plausible deniability," instead of

(…continued)
the plaintiffs are successful, they will extend copyright monopoly to include control over technology, impose unsustainable obligations to restrict designs, chill the development of new technologies and slow the progress of science and the useful arts.") (*quoting* Gary Shapiro, CEA). Of course, nothing in this parade of horribles came to pass after the unanimous Supreme Court decision finding infringement in the Grokster case.

[45] For example, Fred von Lohmann of EFF first condemned copyright owners for suing providers of services that enabled infringing, stating that "if this fight were really about stopping piracy, you would have expected some pirate to actually be sued." Brian Garrity, *Victory Eludes Legal Fight Over File Swapping*, BILLBOARD MAGAZINE (April 13, 2002) (*quoting* Fred Von Lohmann, EFF); Declan McCullagh, *Perspective: End of an era for file-sharing chic?*, CNET (Aug. 25, 2003) (*quoting* Fred Von Lohmann, EFF); Bill Royle, *Interview with EFF's Fred Von Lohmann*, TECHFOCUS NEWS & COMMENTARY, www.techfocus.org (January 2003) ("The Copyright Act, like most of our laws, has been built on the premise that you go after the guy who actually breaks the law…If someone uses a PVR (or computer, or crow bar, or car, for that matter) to break the law, they by all means go after them."). Once copyright owners began to "go after the guy who actually breaks the law" by suing end-users, von Lohmann denounced this strategy as "absurd" and opined that "more lawsuits are not the answer." Fred Von Lohmann, EFF, BOINGBOING (June 25, 2003); Fred Von Lohmann, EFF, *Perspective: RIAA's College Lawsuits a Wrong Answer*, CNET (Sept. 14, 2003); Fred Von Lohmann, EFF, *Op Ed: Copyright Silliness on Campus*, WASHINGTON POST, (June 6, 2007). *Compare also* Gigi Sohn, Public Knowledge, Testimony before the House Judiciary Subcommittee Hearing On "Piracy of Intellectual Property on Peer-to-Peer Networks" (Sept. 26, 2002) ("[A]n industry-initiated lawsuit against a large scale infringer could also have the benefit of serving as a deterrent to other bad actors. As we have seen in other contexts, specifically targeted lawsuits and other legal action can have a deterrent effect, and also educate the public as to what is legal.") and Gigi Sohn, Public Knowledge, *Transcript: Internet Piracy*, WASHINGTON POST (Nov. 5, 2004) ("Again, I have no problem with the movie industry bringing infringement lawsuits *if they are targeted at the most egregious file traders."), *with* Grant Gross, *MPAA to Start Filing Movie-Swapping Lawsuits*, MACWORLD, (Nov. 5, 2004) ("Public Knowledge also firmly believes that simply bringing lawsuits against individual infringers will not solve the problem of infringing activity over P-to-P networks.") (*quoting* Gigi Sohn, Public Knowledge).

[46] Similarly, some groups espoused the position that technology should not be condemned simply because it was used to commit copyright infringement, but later decided that some technologies that could be beneficial in the fight against piracy were inherently evil. *Compare* Scott Cannon, *Justices Poised for Piracy Ruling*, THE KANSAS CITY STAR (May 15, 2005) ("Technologies are not illegal. Actions are illegal") (*quoting* Gigi B. Sohn, Public Knowledge), *with* Gigi B. Sohn, Public Knowledge, Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation on Deep Packet Inspections (Sept. 25, 2008)("It should be clear that the very nature of DPI [deep packet inspection] technology raises grave privacy concerns.").

[47] EFF and Public Knowledge have opposed the PRO-IP Act ("PRO IP Act is just another in a long line of "one-way ratchet" proposals that amplifies copyright without protecting innovators or technology users." - EFF), COICA ("This is a censorship bill that runs roughshod over freedom of speech on the Internet." -EFF), ACTA ("The ACTA juggernaut continues to roll ahead, despite public indignation about an agreement supposedly about counterfeiting that has turned into a regime for global Internet regulation." -EFF), and several of the bills proposed collectively as the Intellectual Property Protection Act, including, the PIRATE Act ("We believe that it is an inappropriate use of federal funds to enforce private rights of action." -Public Knowledge) and the Family Movie Act ("The entertainment industry has hijacked the provision affirming the right of consumers to skip over objectionable material and turned it against consumers and the tech community." -Public Knowledge). *See* EFF, Deeplinks Blog, http://www.eff.org/deeplinks/archive; Public Knowledge, Pending and Enacted Legislation webpage, http://www.publicknowledge.org/legislation.

constructive cooperation, about online copyright theft.[48] These actions undercut any progress toward cooperation. We urge all industry sectors, and the government as well, to stand up against this unproductive and baseless groupthink.

B. Civil litigation

Copyright owners and creators will continue to use the courts to enforce their rights against online copyright theft. We will also actively seek to correct erroneous judicial interpretations that have been made by some lower federal courts, and to advocate for more realistic and practical court interpretations of existing law, and we urge USG to continue to join in that effort. The lawsuits in which we have engaged have had some positive impacts – they have increased public understanding about the consequences of copyright infringement, acted to deter future infringements, and helped shape consumer decision making about seeking legitimate alternatives for the consumption of music.

However, for a number of reasons, the role of lawsuits in solving the online theft problem is clearly limited. For instance, bringing clear-cut claims against major commercial infringers is not by itself a solution in the long run. These cases take years to litigate and are an enormous resource drain. The LimeWire case is indicative of the problem. *Arista Records, LLC v. Lime Group, LLC*, 532 F. Supp. 2d 556 (S.D.N.Y. 2007). It involved an illicit p2p service that was, for all practical purposes, nearly indistinguishable from the service that was on the losing end of the unanimous Supreme Court decision in *MGM v. Grokster*, 545 U.S. 913 (2005). Yet the LimeWire defendants were able to drag out the litigation for 4 years before a federal trial court finally ruled against them in May 2010.[49] Such massive civil cases do not provide a scalable solution to the full scope of the problem.

Enforcing any judgments obtained is also problematic. Online copyright thieves are adept at jumping across borders and assuming alternate identities to evade the long arm of the law.[50] Finally the current restrictions under U.S. law on injunctive relief against intermediaries –

---

[48] *See* Arista Records, LLC v. Lime Group, LLC, 532 F. Supp. 2d 556 (S.D.N.Y. 2007) (describing one attorney's advocating for plausible deniability: "Gorton states that another attorney, Frederick Von Lohman [sic], gave LW . . . confidential legal advice regarding the need to establish a document retention program to purge incriminating information about LimeWire users' activities."); Greg Sandoval, *Did EFF Lawyer Cross Line in LimeWire Case?*, CNET (May 18, 2010) ("During the *Grokster* trial, MGM's lawyers noted that von Lohmann in 2001 wrote a primer called "Peer-to-Peer File Sharing and Copyright Law after Napster." In the piece, von Lohmann advised that to "avoid liability," operators should create 'plausible deniability' by 'choosing an architecture that will convince a judge . . . monitoring and control is impossible.'").

[49] *See Arista Records*, 532 F. Supp. 2d 556.

[50] For example, The Pirate Bay, an illegal Swedish website, was "one of the world's largest facilitators of illegal downloading." David Sarno, *The Internet Sure Loves its Outlaws*, L.A. TIMES (Apr. 29, 2007). In May 2006, the Stockholm headquarters were raided by Swedish police and shut down. However, only three days later, the site was operating once again. The Pirate Bay founders were finally prosecuted in a joint civil and criminal trial in Sweden, and were found guilty of accessory to crime against copyright law in 2009. At the date of the criminal decision against the operators in 2009, the site was obtaining its internet service from a Swedish ISP, PRQ AB. It then moved to another ISP in Sweden, DCA.net, whose business was transferred to a third Swedish ISP, Black Internet, following the bankruptcy of DCS.net. In an attempt to avoid detection and liability via the ISPs, the Pirate Bay did not contract directly with the ISPs but via an intermediary under the name of DCP Networks, which was managed

(…continued)

seeking, for example, an order blocking access to an offshore pirate site – render that remedy almost illusory. Under the DMCA, the only way to obtain such an order – and a very narrow one at that – directed to a service provider that is entitled to safe harbor status is to sue the service provider for copyright infringement, whether direct or contributory. *See* 17 U.S.C. § 512(j). [51] This is precisely the wrong framework within which to encourage, rather than discourage, cooperation by intermediaries against the real target – the offshore pirate site.[52]

C. Criminal enforcement

Federal law enforcement has a critical role to play in the path forward, and has taken some very positive steps against online copyright theft. Notably, the "In Our Sites" initiative took down seven major copyright theft sites through a civil forfeiture action against their registered domain names.[53] On November 29, a much more extensive "In Our Sites II" campaign took down over 80 sites engaged in various forms of intellectual property theft, including online copyright theft, based on the same forfeiture authority.[54]

(…continued)
by one of the operators of The Pirate Bay. The presence of DCP Networks meant that The Pirate Bay did not appear on many of the searches of the internet hosting and IP address allocation arrangements. It also meant the ISP could argue that it was not providing service to The Pirate Bay and that right holders should instead be enforcing their rights against DCP Networks. Although in August 2009, right holders obtained an injunction which prohibited Black Internet from making available copyright works by providing Internet access to The Pirate Bay, the site soon moved to an alternative host in Netherlands. When right holders wrote to this ISP, The Pirate Bay moved to a provider in the Ukraine, and then a provider in Germany. Today, after a Hamburg court issued an injunction prohibiting the German service provider from hosting the site, The Pirate Bay has returned to Sweden.

[51] *See also* Discussion of Stakeholders' Experiences with § 512(j) (Response 2I), Appendix II, at 7.

[52] This is one of several ways in which enactment of legislation like S. 3804 would provide a much more reasonable framework for such cases.

[53] Operation In Our Sites is a joint government effort between the U.S. Immigration and Customs Enforcement (ICE) and the U.S. Attorney General for the Southern District of New York to target Internet counterfeiting and piracy. As ICE Assistant Secretary Morton described, "ICE and our partners at the National Intellectual Property Rights Coordination Center are targeting pirate Web sites run by people who have no respect for creativity and innovation. We are dedicated to protecting the jobs, the income and the tax revenue that disappear when organized criminals traffic in stolen movies for their own profit." For more information on this initiative, see Press Release, ICE, *"Operation In Our Sites" Targets Internet Movie Pirates* (June 30, 2010), http://www.ice.gov/news/releases/1006/100630losangeles.htm.

[54] Operation in Our Sites II is a joint government effort between the Justice Department's Criminal Division, the Department of Homeland Security, and several U.S. Attorneys' Offices nationwide. This joint effort targets online retailers engaged in the sale and distribution of counterfeit goods, ranging from sporting equipment, to handbags, to illegal copies of DVDs and music. As Attorney General Eric Holder remarked, "The Justice Department's commitment to IP enforcement has never been stronger. This work is a top priority. And through the leadership of the Department's Criminal Division and our U.S. Attorneys' Offices – and with the help of ICE, the FBI, and many other agency and law enforcement partners – we will continue our efforts to protect intellectual property rights and to disrupt markets for counterfeit or infringing goods." For more information on Operation in Our Sites II, see Remarks of Attorney General Eric Holder, Press Conference on Operation in Our Sites II (Washington, D.C. Nov. 29, 2010), http://www.justice.gov/iso/opa/ag/speeches/2010/ag-speech-101129.html.

The National Intellectual Property Rights Coordination Center led by ICE's Office of Homeland Security Investigations has been a model of interagency cooperation, and its investigations have to date led to the seizure of 100 websites dedicated to selling or distributing infringing content and the seizure of hundreds of thousands of counterfeit DVDs and counterfeit CDs. The federal agencies involved in this effort deserve significant credit for recognizing the incredible damage done to our economy by intellectual property theft and taking aggressive action to seek justice.

Overall, however, resource constraints have limited the scale of the federal criminal response. Law enforcement agencies should be directed to continue to make aggressive use of existing authorities, but they also need more resources and some new legal tools if their efforts are to begin to match the scale of the problem.

D. Legislation

To the extent that voluntary agreements and further litigation do not enable meaningful and improved enforcement given the realities of online copyright theft in the 21st century, adjustments to the law may need to be considered, to ensure that the incentives for cooperation are strong enough to produce the needed results.

In addition, the existing legal landscape should be supplemented by enactments along the lines of S. 3804, the Combating Online Infringement and Counterfeits Act. This legislation addresses the highly visible and especially destructive phenomenon of websites dedicated to copyright theft. These sophisticated sites, which sometimes feature advertising from major corporations and the logos of respected financial transaction service providers, often appear legitimate to many consumers; but they do little but offer pirate versions of copyrighted movies, TV shows, musical recordings, videogames, e-books, and other works. While hardly the only example of online copyright theft, the high-volume activities of these sites contribute significantly to the damage inflicted by online theft as a whole.

S. 3804 offers a balanced, appropriate, and much needed supplement to the existing legal arsenal that can be deployed against these egregious online theft sites. Through focused definitions and carefully circumscribed remedies, S. 3804 enables expeditious, effective and constitutionally sound action against sites dedicated to piracy, wherever they are located. It will have no adverse impact on principles of Internet architecture, respects the sovereignty of other countries over the operation of their own domain name registries, and provides a model for sound but targeted legal rules that will help the Internet fulfill its promise to consumers and citizens as well as to creators. Its enactment should be made a top priority.

V. Conclusion

We commend DOC for this NOI. We believe that an objective examination of facts will amply demonstrate that the current system is not working to protect our creators, our economy, our culture, or our jobs. We hope that this proceeding will mark a first step toward re-striking the balance, with greater cooperation among the key players, better legal tools, and a more productive approach to this pervasive and pernicious problem.

Respectfully submitted,

American Association of Independent Music (A2IM)
American Federation of Musicians of the United States and Canada (AFM)
American Federation of Television and Radio Artists (AFTRA)
Directors Guild of America (DGA)
International Alliance of Theatrical and Stage Employees (IATSE)
Motion Picture Association of America (MPAA)
National Music Publishers' Association (NMPA)
Recording Industry Association of America (RIAA)
Screen Actors Guild (SAG)

December 10, 2010

APPENDIX I

DESCRIPTIONS OF CREATIVE COMMUNITY ORGANIZATIONS

1. A2IM

American Association of Independent Music ("A2IM") is a 501 (c) (6) not-for-profit trade organization that represents a broad coalition of independent music labels, a sector that comprised more than 38% of digital sales of recorded music in 2009. A2IM represents Independent music label's interests in the marketplace, in the media, on Capitol Hill, and as part of the global music community. A2IM's music label community includes music companies of all sizes throughout the United States, representing musical genres as diverse as its membership. All of A2IM's members should be considered small and medium-sized enterprises with limited resources to fight piracy and all are small business people with a love for music who are trying to make a living. A2IM members share the core conviction that the independent music community plays a vital role in the continued advancement of cultural diversity and innovation in music.

2. American Federation of Musicians of the United States and Canada

The American Federation of Musicians of the United States and Canada (AFM) is the largest union in the world representing professional musicians, with over 80,000 members in the United States and Canada. Musicians represented by the AFM record music for sound recordings, movie sound tracks, commercials, and television and radio programming under industry-wide collective bargaining agreements. The AFM works to ensure that musicians not only receive fair wages and benefits, but also participate in the proceeds from the sale or other exploitation of their recorded performances in physical or digital formats, and have a voice in cultural and policy debates that affect them at home and abroad.

3. American Federation of Television and Radio Artists

AFTRA members are the people who entertain and inform America and work as actors, singers, journalists, dancers, announcers, comedians, disc jockeys and other performers in television, radio, cable, sound recordings, music videos, commercials, audiobooks, non-broadcast industrials, interactive games and all formats of digital media. Founded in 1937, AFTRA today provides its more than 70,000 members nationally a forum for bargaining strong wages, benefits and working conditions and the tools and upward mobility to pursue their careers with security and dignity. From new art forms to new technology, AFTRA members embrace change in their work and craft to enhance 21st century American culture and society.

4. Directors Guild of America

DGA was founded in 1936 to protect the economic and creative rights of Directors. Over the years, its membership has expanded to include the entire directorial team, including Unit Production Managers, Assistant Directors, Associate Directors, Stage Managers, and Production Associates. DGA's 14,600 members live and work throughout the U.S. and abroad, and are vital contributors to the production of feature films, television programs, documentary features, news and sports, commercials, and content made for the Internet and new media. DGA seeks to

protect the legal, economic, and artistic rights of directorial teams, and advocates for their creative freedom.

5. International Alliance of Theatrical Stage Employees

IATSE is the labor union that represents technicians, artisans, and craftspersons in the entertainment industry, including live theater, motion picture and television production, and trade shows. IATSE was formed in 1893 and has over 110,000 members. Through its international organization and its autonomous local unions, IATSE seeks to represent every worker employed in its crafts and to help them obtain the kind of wages, benefits, and working conditions they need for themselves and their families.

6. Motion Picture Association of America

The Motion Picture Association of America, Inc. (MPAA) serves as the voice and advocate of the American motion picture, home video and television industries from its offices in Los Angeles and Washington, D.C. Its members include: The Walt Disney Studios; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLLP; and Warner Bros. Entertainment Inc.

7. National Music Publishers' Association

Founded in 1917, the National Music Publishers' Association (NMPA) is the trade association representing over 2,500 American music publishers and their songwriting partners. The NMPA's mandate is to protect and advance the interests of music publishers and songwriters in matters relating to the domestic and global protection of music copyrights.

8. Recording Industry Association of America

The Recording Industry Association of America is the trade group that represents the U.S. recording industry. Its mission is to foster a business and legal climate that supports and promotes our members' creative and financial vitality. Its members are the record companies that comprise the most vibrant national music industry in the world. RIAA® members create, manufacture and/or distribute approximately 85% of all legitimate sound recordings produced and sold in the United States.

In support of this mission, the RIAA works to protect intellectual property rights worldwide and the First Amendment rights of artists; conduct consumer industry and technical research; and monitor and review state and federal laws, regulations and policies. The RIAA® also certifies Gold®, Platinum®, Multi-Platinum™, and Diamond sales awards as well as Los Premios De Oro y Platino™, an award celebrating Latin music sales and its new Digital Sales award.

9. Screen Actors Guild

SAG is the nation's largest labor union representing working actors. Established in 1933, SAG has a rich history in the American labor movement, from standing up to studios to break long-term engagement contracts in the 1940s, to fighting for artists' rights amid the digital revolution sweeping the entertainment industry in the 21st century. With 20 branches nationwide, SAG represents over 120,000 actors who work in film and digital motion pictures, television programs, commercials, video games, industrial shows, Internet, and all new media formats. SAG exists to enhance actors' working conditions, compensation, and benefits and to serve as a powerful unified voice on behalf of artists' rights.

BEFORE THE

OFFICE OF THE SECRETARY, U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE, U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION,
U.S. DEPARTMENT OF COMMERCE

Regarding:

Notice of Inquiry on "Copyright Policy, Creativity, and Innovation in the Internet Economy"
75 Fed. Reg. 61419 (Oct. 5, 2010)
[Docket No. 100910448–0448–01]

Appendix II: Responses to Specific Questions in the NOI

Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy

(p. 61422)

1. Rights Holders: Protection and Detection Strategies for Online Infringement

1A. What are stakeholders' experiences and what data collection has occurred related to trends in the technologies used to engage in online copyright piracy, and what is the prevalence of such piracy?

A. The technologies currently used to disseminate illegally copied motion picture, television and music content online include, but are not limited to:

- *Video on Demand Streaming: These websites include those which provide users the ability to watch illegal copies of movie, television and music video content for free without installing a program or first downloading a complete file. Streaming websites allow users to click and instantaneously view content streamed to their computer.*

- *Audio Only on Demand Streaming: These websites include those which provide users the ability to stream sound recordings for free at any time without any compensation to the artist or copyright holder. By contrast, licensed on-demand music streaming services may be free to the user, but the service pays compensation for the use of the music.*

- *Peer-to-Peer: These networks enable users to download complete copies of illegally copied movie, television and music content for free using a "client" program installed on their own computer. The client program facilitates the simultaneous download of an illegal movie or television file, or an album or artist collection of*

music, from other users in small, quickly downloaded parts, as well as the quick download of individual sound recording files.

- *Direct Download: These include websites that permit users to download illegally copied movie, television and music content either on a per download charge, subscription charge, or advertising-supported basis. This can include illegal online storefronts and/or so-called locker services, etc.*

- *Usenet: Usenet allows the distribution of music, movie and television content through a series of connected news servers. Users subscribe to paid news group services to access illegal music, movie and television content stored on Usenet servers around the world.*

- *Linking Sites: These include websites or webpages that announce and provide multiple direct links to lockers or servers where movies, television and music content can be illegally streamed or downloaded.*

- *Search and Stream/Download: These include websites or applications, including recently several illicit mobile applications available via the Android marketplace and similar platforms, that permit a user to search for a specific song, album, show, or movie and then link them to a site where such content can be illegally obtained. Often these applications are marketed and optimized to search for either just mp3 music files, or files from a particular artist, etc. In the mobile context, these applications may include a sharing feature to promote further illegal distribution of the file.*

- *Online Marketing of Physical Counterfeit Products: These websites are used to illegally, market, offer, sell, distribute and collect payment for physical counterfeit copies of music, television shows and movies.*

Recently, there has been a significant rise of illegal on-demand streaming and illegal direct downloads from so-called digital lockers among other means, as well as a rise in illicit mobile applications that facilitate online theft.[1] *In addition, p2p applications still account for a significant share of unauthorized dissemination of stolen content. This trend is confirmed by studies of overall network traffic patterns. For instance, the October 2010 Cisco Visual Networking Index report found p2p file sharing declined to 25% of global broadband traffic, although it is still growing in absolute terms. Cisco Systems Visual Networking Index (Oct. 2010). Another recent study by Sandvine found that p2p filesharing "accounts for 37% of all bytes carried, and that BitTorrent is the dominant application. Sandvine, Fall 2010 Global Internet Phenomena Report, at 15 (2010) Another study by Professor Ed Felten found that 99% of the BitTorrent traffic concerning movies appeared to be infringing. Ed Felten, Census of Files Available via BitTorrent, FREEDOM TO TINKER (Jan. 29, 2010), http://www.freedom-to-tinker.com/blog/felten/census-files-available-bittorrent. One Australian study found, after evaluating more than one million torrents on BitTorrent networks, that 97.9% of non-*

[1] *See infra*, response to Question 1E below.

pornographic files were infringing copyright. Robert Layton and Paul Watters, Internet Commerce Security Laboratory, Investigation into the Extent of Infringing Content on BitTorrent Networks, at 21 (April 2010).

1B. What new studies have been conducted or are in-process to estimate the economic effects of this piracy?

A. A number of such studies were cited and summarized in the creative community organizations' submission to the U.S. Intellectual Property Enforcement Coordinator in March 2010. Letter from Creative Community Organizations to the Honorable Victoria A. Espinel, United States Intellectual Property Enforcement Coordinator (Mar. 24, 2010), at 3-4, available at http://www.mpaa.org/Resources/0c72c549-89ce-4815-9a71-de13b8e0a26f.PDF. We are not aware of any new studies undertaken since that time.

1C. What assumptions are made in such studies on the substitution rates among the different forms of content?

A. In several academic studies regarding peer-to-peer file sharing of music, substitution rates of up to 30% have been demonstrated. One study by Stan Liebowitz found, on average, a decline in music sales of 8-9% during the years in which Napster was most popular. Stan Liebowitz, File Sharing: Creative Destruction or just Plain Destruction?, 49 J. Law & Econ. 1, 15 (2006). Another study found that between 2000 and 2003, music industry revenue decreased by 16%. Rafael Rob and Joel Waldfogel, Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College Students, 49 J. Law. & Econ. 29 (2006). More specifically, between 1999 and 2003, the estimated sales displacement of hit albums (those selling at least 2 million), due to unauthorized downloads, ranged between 17-19% for college students (depending on school). Id. at 46. In just 2003 alone, the displacement estimate was 9%. Id. at 47. Yet another study found a much higher impact of peer-to-peer sharing on music sales. Alejandro Zentner found that peer-to-peer file sharing "reduces the probability of buying music" by up to 30%. Alejandro Zentner, Measuring the Effect of File Sharing on Music, 49 J. Law. & Econ. 63.

1D. What technologies are currently used to detect or prevent online infringement and how effective are these technologies?

A. A range of such technologies are readily available in the marketplace from companies such as (but not limited to) Audible Magic, Enterasys, Mirage Networks and Red Lambda. In general, there are several technologies and methods that can be used by network administrators and providers, including many that are already used for spam and virus protection. These include:

- *Technologies to detect, monitor (and filter) traffic or specific files based on analysis of information such as protocols, file types, text description, metadata, file size and other "external" information;*

- *Content recognition technologies such as digital hashes, watermark detection, and fingerprinting technologies;*

- *Site blocking, redirection with automated warning systems/quarantine of repeat offending sites and/or IP addresses / locations from which repeat infringing activity has occurred;*

- *Bandwidth shaping and throttling;*

- *Scanning infrastructure (the ability to subscribe to RSS-style data feeds as sites get new postings of content and links (for linking, streaming, and locker sites); and*

- *Consumer tools for managing copyright infringement from the home (based on tools used to protect consumers from viruses and malware).*

1E. What observations, if any, have been made as to patterns of online infringement as broadband Internet access has become more available?

A. As noted above, there appears to be a trend towards various forms of illegal streaming and direct downloading. Another disturbing trend, which parallels the growth of legitimate online sources for digital content, is the emergence of sophisticated online theft sites that adopt the "look and feel" of the legitimate outlets. These sites include advertisements from major mainstream companies and offer transactions through mainstream payment services and credit cards. In addition, as mobile broadband becomes more mainstream, we are seeing a large increase in the number of mobile applications that facilitate copyright infringement. For example, in 2010 alone, RIAA has identified, and sent notices concerning, more than 250 such applications.

1F. Is litigation an effective option for preventing Internet piracy?

A. See discussion in text of the submission.

1G. Consistent with free speech, due process, antitrust, and privacy concerns, what incentives could encourage use of detection technologies by online services providers, as well as assistance from payment service providers, to curb online copyright infringement?

A. See discussion in text of submission. We look forward to reviewing the answers of online services providers and payment services providers to this question.

1H. What challenges have the creative industries experienced in developing new business models to offer content online and, in the process, to counteract infringing Internet downloads and streaming?

1I. Can commenters make any generalizations about the online business models that are most likely to succeed in the 21st century, as well as the technological and policy

decisions that might help creators earn a return for their efforts? (Again, keeping in mind free speech, due process and privacy concerns.)

1J. How can government policy or intellectual property laws promote successful, legitimate business models and discourage infringement-driven models?

1K. And, how can these policies advance these goals while respecting the myriad legitimate ways to exchange non-copyrighted information (or the fair use of copyrighted works) on the Internet?

A. (to questions 1H-1K): As discussed in the text of the submission, the major problem encountered by the creative industries in developing new business models for delivery of content online is the presence in the same marketplace of vast quantities of illicit and unlicensed copies of the same content, which is offered to consumers either for free, or at a price that reflects the parasitic character of these online sources, which incur none of the costs shouldered by legitimate producers and distributors. Despite this overwhelming challenge, a wide variety of licensed and legitimate sources now offer a huge volume of content to online consumers in an unprecedented range of media, delivery methods, license terms and price points. See, for example, the wide variety of legitimate online sources for movies and television programs listed at http://www.respectcopyrights.org/getmovies.html, and the wide variety of legitimate online music sources listed at http://www.riaa.com/toolsforparents.php?content_selector=legal_music_sites, www.pro-music.org and at www.musicunited.org.[2] See also our response to Question 3A below regarding the various educational resources available to education the public about copyright, and legal alternatives for obtaining the music, movies and television shows they want.

Government policy and intellectual property laws can best foster successful, legitimate business models by encouraging cooperation among all industry players to detect and deal with online theft; by removing any impediments to such cooperation that may arise from other areas of the law; by facilitating private enforcement of copyright laws in the online environment, both in the US and overseas; and, where appropriate, by bringing targeted criminal enforcement actions against egregious offenders. Such a policy will have limited if any impact upon fair use of copyrighted works or the legitimate online exchange of un-copyrighted material. While there are certainly significant legal issues concerning the application of the fair use doctrine and other limitations to copyright in the online environment, the online theft that is most injurious to creators, copyright owners, and the U.S. economy and culture as a whole, falls far outside the scope of any plausible fair use claim. Further details are provided in the text of the submission.

[2] As noted in the main submission, today there are more than 11 million legal tracks available online and nearly 400 legitimate services worldwide for the consumption of music, as compared to 1 million tracks and fewer than 50 services in 2003. Today there are legitimate services through which a user can stream music to his phone, purchase the music on the fly, have music available "off the grid" for when the user is not connected to the internet, and listen to Pandora through their television, car or computer.

2. Internet Intermediaries: Safe Harbors and Responsibilities

(p. 61423)

2A. What are stakeholders' experiences with the volume and accuracy of takedown notices issued for allegedly infringing content across the different types of online services (i.e., storage, caching, and search) and technologies (e.g., p2p, cyber lockers, streaming, etc.)?

A. A high volume of takedown notices is the norm because of the high volume of online copyright theft. In the first ten months of 2010, IFPI, the international recording industry body, sent 146,593 notices to service providers regarding 5,816,847 links to infringing recordings across a variety of online services. In that time, IFPI has received fewer than 60 counter-notices. Similarly, RIAA has sent millions of notices to commercial ISPs concerning p2p infringements by their subscribers, and received relatively few counterclaims regarding the accuracy of such notices.[3]

NMPA publishers who participate in its notice and takedown program ("N&T Program" have never received counter-notices in response to the notices sent through the program. The N&T Program began first only to combat illegal guitar tab uses, but has since been expanded to include illegal lyrics and sheet music uses. During the course of the program, hundreds of notices identifying thousands of works have been sent.

The experience of the MPAA and its members (who, in aggregate, also send millions of notices to commercial ISPs) is similar. We believe that ensuring that individual cases are identified, using robust methodologies, results in a minimal number of questions from ISPs or their subscribers regarding the validity of notices and that our methodologies meet or exceed the "good faith belief" standard of the DMCA..

2B. What processes are employed by rights holders to identify infringers for purposes of sending takedown notices?

A. The major copyright industry enforcement bodies have developed over the years extensive protocols to verify the accuracy of takedown notices they send. As a result, the rate of false positives is believed to be extremely low. A few celebrated cases of inaccurate notices have become noteworthy precisely because they are so rare, and should play little role in fashioning a data-driven policy in this area. Other techniques may include the use of metadata matching or watermarking to identify stolen content.

The MPAA has contributed to the development and deployment of - and has adopted - a comprehensive set of published technical standards, that are intended to ensure that infringements detected on p2p networks are validated fully, and confirmed to be associated with illegal copies of MPAA member content. These standards extend the already existing set of Automated Copyright Notification System (ACNS) messages and also incorporate standards for

[3] Please note this volume of notices is limited by, among other things, the resources the rights holders have to combat such theft. We estimate that the actual volume of infringement is much higher than what is identified through our current processes.

identifying and verifying the content itself and the IP address that is sharing the content. For more information, see www.acns.net. Pursuant to these standards, notices communicated to ISPs for forwarding to ISPs' subscribers are supported by comprehensive evidence packages. The results of this detection methodology have been presented already and have been accepted in several legal proceedings. For example, in Roadshow Films Pty Ltd. v. iiNet Ltd., a case before the Federal Court of Australia, the court thoroughly examined the evidence of the methods used to identify infringing material and found that the evidence, including DetecNet's hash verification methods, "established beyond doubt that a particular file has corresponded with a film of the applicants."

In collecting evidence for p2p notices, investigators from RIAA's vendor usually use special software to check the "hash," a sort of unique digital fingerprint, of each offered file to verify that it is identical to a copyrighted song file in the RIAA's database. In the rare cases in which the hashes don't match, the investigators download the song and use fingerprinting technology to compare the sound waves of the offered audio file against those of the song it may be infringing upon. If the fingerprinting technology still doesn't turn up a match, then a live person will listen to the song. If there is a match, investigators will then engage in a so-called TCP connection, or an electronic "handshake," with the computer that is offering the file to verify that the computer is online and is ready to share the song. (See http://chronicle.com/article/How-It-Does-It-The-RIAA/786/ for a published account of RIAA's methodology that remains essentially accurate.)

For movie and TV files (more often found on BitTorrent networks), the detection and verification processes also use hashes and reference files to confirm that identified versions of content are infringing When a file with a so-far not seen hash or set of unique identifying criteria is detected (for example because a new illegal version has been posted), a complete copy of the content is downloaded and both manual (i.e. human) and automated (e.g. proven fingerprinting tools) means are deployed to confirm that the file is, or is not infringing. For any vendor engaged by the MPAA, it is a contractual requirement that EVERY infringement is verified using published and comprehensive methods before any notice would be generated and forwarded to an ISP. It is important to note that hash verification and some of the other methodologies used to confirm content status on p2p networks are also used to assist analysis and to confirm the status of files found in other environments (UGC sites, Cyberlockers etc.).

NMPA, on behalf of its nearly 2,600 publisher members, engages special outside legal counsel to administer its N&T Program directed at unauthorized use of guitar tabs, lyrics, and sheet music on the Internet. NMPA's counsel undertakes stringent research and authorization process necessary before a notice can be sent. As the N&T Program is focused on written uses of publishers' works, NMPA's counsel on a regular basis conducts text searches of publishers' works on the internet – a time consuming and expensive manual process. NMPA's counsel then alerts the publishers to the infringing use and is granted the necessary permissions to send DMCA takedown notices. NMPA publishers also notify NMPA of illegal uses of their works, which are provided to NMPA's counsel for verification and action. NMPA's counsel next must identify the registrants and ISPs of the sites, which is often difficult, since many infringing sites employ services such as "Domains By Proxy" and "Front Registrant" to elude such identification.

Outside the N&T Program, NMPA publishers have employed third party vendors who use specialized computer programs and dedicated personnel to systematically search voluminous amounts of audio visual content on the internet. That vendor then seeks verification of ownership and the requisite permission of works identified as infringing from these publishers to authorize them to send DMCA takedown notices. For many songwriters and smaller music publishing companies, however, individually undertaking this process is cost prohibitive.

2C. What processes do Internet intermediaries employ in response to takedown notices?

A. While some service providers offer a convenient interface for the automated processing of takedown notices, the policies of others are clearly designed to discourage the submission of takedown notices. For example, Twitter, a company whose entire business is online, does not accept any DMCA takedown notices via e-mail or any other form of electronic communication. It ignores notices sent by any other means but U.S. mail or fax. (An example of Twitter's response to a DMCA notice is appended to this response.) In other cases, intermediaries have placed limits on the number of infringement notices that they will accept, or asked for or demanded additional information not required by the DMCA before processing an infringement notice.

2D. Are Internet intermediaries' responses to takedown notices sufficiently timely to limit the damage caused by infringement?

2E. What are the challenges of managing this system of notices?

A (to questions 2D-2E). Generally no. For instance, 8,381 links were sent to Google for de-listing by the British Phonographic Industry in July through October 2010. On average it took one to two days for Google to acknowledge the request, and another 5 days for the link to be removed. In a hit-driven business, the availability of stolen content through the world's largest search engine for one week cannot be considered an effective system. This is especially true in the case of pre-release material. In light of these concerns, we acknowledge that Google has announced plans to decrease processing speeds, and we welcome that development. However, we also note that at least a handful of service providers provide nearly instantaneous takedowns, thus more can and should be done.

In addition, RIAA reports worrisome response times of several days to weeks to requests to remove infringing mobile applications from storefronts, and a disturbing trend to either ignore such requests or refuse to remove such applications.

With certain exceptions, it has been NMPA's experience that many ISPs and search engines have chosen to interpret the DMCA narrowly and have not taken down repeat infringers or delinked such infringing sites when presented with repeated evidence of infringement. Instead, some ISPs and search engines have merely removed the samples of infringement and taken the position that that is the limit of their legal obligations under the statute.

2F. What are stakeholders' experiences with online copyright infringement by users who change URLs, ISPs, locations, and/or equipment to avoid detection?

2G. What challenges exist to the identification of such systematic infringers?

A (to questions 2F-2G). In relation to the operators of infringing services, The Pirate Bay is an example of the lengths a service will go to in order to avoid enforcement action. Despite criminal and civil decisions against the operators and one of the site's former hosting providers, The Pirate Bay continues to be able to find ISPs willing to host the site, and has moved through countries including Sweden, the Netherlands, Ukraine and Germany.

At the date of the criminal decision against the operators in April 2009, the site was obtaining its internet service from a Swedish ISP, PRQ AB. It then moved to another ISP in Sweden, DCS.net, whose business was transferred to a third Swedish ISP, Black Internet, following the bankruptcy of DCS.net. In an attempt to avoid detection and liability via the ISPs, The Pirate Bay did not contract directly with the ISPs but via an intermediary under the name of DCP Networks, which was managed by one of the operators of The Pirate Bay. The presence of DCP Networks meant that The Pirate Bay did not feature on many of the searches of the internet hosting and IP address allocation arrangements. It also meant the ISP could argue that it was not providing service to The Pirate Bay and that right holders should instead be enforcing their rights against DCP Networks. DCP Networks was not registered as a corporate entity in Sweden and no contact details other than an email address for the organisation could be found.

In August 2009, right holders obtained an injunction which prohibited Black Internet from making available copyright works by providing Internet access to The Pirate Bay. Black Internet complied with the prohibition and the main portal and tracker went offline temporarily. However, the site soon moved to an alternative host in the Netherlands, Patrickweb. Right holders wrote to this ISP and The Pirate Bay moved to a provider in the Ukraine for a short period before moving on to a provider in Germany, CB3Rob. CB3Rob hosted the site until May 2010, when a Hamburg court issued an injunction prohibiting it from providing internet connection services to The Pirate Bay. The site has now returned to Sweden.

While the Pirate Bay is a high profile example, there is a "hard core" of other BitTorrent sites that use similar means to avoid detection and that move from one ISP and jurisdiction to another to avoid enforcement. In some cases right holders have sought to obtain disclosure of user details from the host ISPs – ISPs are usually reluctant to provide these, and often when they do, the details are meaningless because they name corporate entities that cannot be traced and may not exist.

2H. What are stakeholders' experiences with Section 512(i) on the establishment of policies by online service providers to inform subscribers of service termination for repeat infringement?

A. First, we note that the requirement under 17 USC § 512(i) is not simply to inform subscribers about repeat infringer policies, but in fact to "reasonably implement" them. Our concerns are focused on the latter obligation rather than the former. While there are some

exceptions, we believe that the policies that are actually implemented fall well short of being effective to communicate that there will be adverse consequence for those who choose to "repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others." H. Rept. 105-551 (Part II), Report of House Commerce Committee on H.R. 2281, the Digital Millennium Copyright Act (July 22, 1998), at 61. This is extremely difficult to determine with regard to end-user subscribers to ISP, web hosting, or other intermediary services, since only the service providers have access to the information correlating notices from copyright holders with specific subscribers. However, the policies of some intermediaries needlessly obstruct the implementation of reasonable policies. Examples include purging their IP assignment logs after short periods such as 45 days, or collecting insufficient information from subscribers so that it is impossible to identify them should they open a new account to avoid detection of infringing activity.

Furthermore, in the case of some services such as blogs that repeatedly provide links to infringing material, there is concrete evidence of the shortcomings of existing policies. It is not unusual for blogs to remain active even after 6-10 notices have been delivered to the hosting provider about abusive postings. IFPI routinely alerts Google that certain blogs have been the subject of multiple take down notices. Of the 392 blog "repeat infringer" notices sent by IFPI , 381 were removed by Google; but many remained accessible for as long as 50 days before they were removed. The remaining 11 blogs were still live, some of which remained accessible for over 150 days since IFPI's original repeat infringer notice, despite follow up notices being sent.

As another example, NMPA notes the issues with ThePlanet, an ISP based in Dallas. ThePlanet hosts the largest and most successful offshore illegal lyric sites. ThePlanet serves tens of millions unique visitors monthly viewing hundreds of millions of illegal lyric pages monthly. NMPA has sent dozens of take down and repeat infringer notices to ThePlanet regarding these sites. Each notice identifies an additional 10 to 20 new infringements. ThePlanet's counsel has advised regularly that these sites are repeat infringers and will take the sites down. Not one of the sites has ever come down. Rather, ThePlanet takes down the sample songs only and directs users looking for the removed lyrics to another illegal site still offering the lyrics. Nor, in NMPA's experience, has any other ISP taken down a repeat infringer during the four years of NMPA's anti-piracy program. The illegal sites that have come down have done so voluntarily, as a result of litigation or have taken a license.

2I. What are stakeholders' experiences with the framework in Section 512(j) for injunctive relief to prevent or restrain online infringement?

A. As discussed in the text of the submission, 17 USC § 512(j) is of little value in the fight against online copyright theft. In the only case in which the recording industry has sought to invoke this provision to obtain an order directing an ISP to block access to an offshore pirate site, the response from ISP's counsel was to deny that the Copyright Act "provides any basis whatsoever for such an order." This reaction has created a Catch 22 situation in which service providers refuse to block access to even the most blatant and indefensible online theft sites without a court order, and then deny that courts can issue such an order unless the ISP can be proven guilty of copyright infringement. Among other things, the pending legislation (S. 3804)

regarding sites dedicated to online copyright infringement will clarify the power of courts to issue such orders in appropriate circumstances.

2J. Would stakeholders recommend improvements to existing legal remedies or even new and additional legal remedies to deal with infringing content on a more timely basis?

A. Yes. We believe that S. 3804 contains the main elements for providing an expeditious and effective remedy, consistent with due process and protection for freedom of expression, against at least the most egregious examples sites that are clearly dedicated to stealing copyrighted material and making it available without compensation. Other legislative adjustments that we believe should be considered are summarized in the text of the submission.

2K. What are stakeholders' experiences with developing collaborative approaches to address online copyright infringement?

2L. What range of stakeholders participated in the development of such collaborative approaches?

2M. Have collaborative approaches resulted in the formulation of best practices, the adoption of private graduated response systems, or other measures to deter online infringement that can be replicated?

2N. What other collaborative approaches should stakeholders consider?

2O. How can government best encourage collaborative approaches within the private sector?

2P. In confronting the challenges of online content and copyright infringement, to what extent have all relevant stakeholder groups, such as independent creators and Internet users, participated in or had a window on collaborative approaches to curb online infringement?

2Q. Recognizing the inherent challenges in engaging a wide variety of stakeholders—large and small, noncommercial, multinational (among others)—in such collaborative approaches, what strategies, if any, have been used to collect third-party input and feedback or communicate the outcomes to users and other nonparticipating stakeholders?

2R. For those engaged in collaborative efforts to protect copyrighted works, what are the practical challenges, if any, in promoting transparency, inclusiveness, clarity in expected behavior, and fair process for end users?

2S. Are there examples of voluntary arrangements that effectively meet these challenges?

A (to questions 2K-2S). As discussed in detail in the main submission, there are a few well-publicized examples of successful cooperative efforts to address online copyright infringement, and there have also been a limited number of other productive discussions. What the NOI refers to as "private graduated response systems" have been implemented by a number

of institutions of higher education, as discussed in the main submission, and by some commercial ISPs,[4] and we believe that similar programs should be implemented at other universities and provide a useful model for adaptation to other contexts as well.

We certainly agree that the perspectives of independent creators, as well as of the men and women who depend for their livelihoods on the creation, production and dissemination of creative works, must be considered in the development of these cooperative initiatives, as well as the impact such programs will have on users. However, incorporating the perspectives of Internet users is a difficult challenge, especially since some organizations purporting to represent such perspectives reflexively oppose all effective measures taken to combat online copyright theft.

In the view of the creative community organizations, the interests of consumers and Internet users in this area are best served by an policy that maximizes the opportunities for dissemination of creative works online in a competitive marketplace that is also well safeguarded against online copyright theft and other forms of Internet-based crime and misconduct. We also recognize that consumer acceptance and support is essential for achieving these goals, and have repeatedly demonstrated that, as businesses that live and die in the consumer marketplace, we approach these issues with flexibility and a spirit of experimentation. Business models for online delivery of creative content have already undergone dramatic change in response to consumer needs, desires and preferences, and will undoubtedly continue to do so. The ability to respond flexibly to consumer demands will only be enhanced in a safer, better-lit marketplace in which the role of purveyors of stolen goods and misappropriated services is marginalized.

3. Internet Users: Consumers of Online Works and User-Generated Content

(p. 61423-61424)

3A. What initiatives have been undertaken to improve the general awareness of Internet users about online copyright infringement and the availability of legitimate sources to access online copyrighted works?

A. Copyright owners have undertaken a number of efforts in this area. See, for example, the educational materials prepared by the Copyright Alliance Educational Foundation, at http://www.copyrightfoundation.org/; material for parents at http://www.musicunited.org/9_parents.aspx and at http://www.riaa.com/toolsforparents.php; educational links collected at http://www.musicunited.org/10_education.aspx and at http://www.riaa.com/toolsforparents.php?content_selector=tools_pe_educators; material at

[4] *See e.g.*, Greg Sandoval, *Cable One: Unsecured Network won't Excuse Piracy*, CNET (Nov. 10, 2010), *available at* http://news.cnet.com/8301-31001_3-20022424-261.html?tag=cnetRiver; Ernesto, *US ISP Disconnects Alleged Pirates for 6 Months*, TORRENTFREAK (Sept. 24, 2010), *available at* http://torrentfreak.com/us-isp-disconnects-alleged-pirates-for-6-months-100924/.

http://www.respectc opyrights.org/, including links to many legitimate sources of online movies and TV shows. In the UK, the Music Matters trustmark campaign is an effort to certify legitimate sources for online music. See http://whymusicmatters.org/what-music-matters-campaign.

3B. What are stakeholders' experiences with the awareness and appropriate use by Internet users of the counter-notification mechanism?

3C. What are stakeholders' experiences regarding inappropriate use by Internet users of the counternotification mechanism, if any?

3D. What are stakeholders' experiences with the volume of counter-notices filed?

A. (to questions 3B-3D). Our experience is that very few counter-notifications are filed. This outcome is consistent with the care taken to maintain quality control on the sending of notices. For example, the nearly 150,000 notices sent by IFPI in 2010 to date have resulted in fewer than 60 counter-notices. Furthermore, many counter-notifications received were unfounded, inappropriate, or provide no reason for believing that the takedown was the result of "mistake or misidentification," the only appropriate grounds for a valid counter-notification under the statute. Some are not even counter-notifications at all. For instance, see the report regarding Ellen Seidler, co-producer of the widely stolen film "And Then Came Lola" discussed in the text of this submission, in which Google apparently treated as a valid counter-notification a message from a Chinese site operator (for which Google was serving advertisements) admitting that the streaming of the film was unauthorized. See http://blog.copyrightalliance.org/2010/09/google-ads-on-rogue-sites/.

3E. Do current methods of detecting infringement affect consumers' ability to legally obtain copies of copyrighted works and/or share legal user-generated content?

A. No.

3F. What are the experiences of universities in raising general awareness with their communities about the harms of digital piracy?

3G. What are stakeholders' experiences in foreign countries and on university campuses in reducing online copyright infringement?

A (to questions 3F-3G). See discussion in text of submission with regard to universities. With regard to foreign countries, many of the educational initiatives listed on response to question 3A are international in scope. Additionally, in several countries where efforts to promote voluntary cooperation between right holders and service providers have fallen short, governments have enacted, or are considering, laws or regulations that mandate more robust policies against repeat infringers, including in several cases "graduated response" requirements.

3H. In turn, are independent creators and Internet users able to fully exploit the Internet platform for the distribution of their works and, if not, what barriers have been encountered?

A. No, they are not, and lack of effective protection for their intellectual property rights is the main barrier encountered. Besides the examples provided in the text of our submission, we call your attention to the submission made by A2IM (the American Association of Independent Music) in docket number ITA–2010–0006. As noted by A2IM, whose membership consists entirely of small and medium sized enterprises (SMEs) seeking to make a living in the music business:

> *"Over the course of the past decade, dramatic shifts in technology have impacted nearly every aspect of the music industry, from the recording and distribution of sound recordings to the cultivating of audiences for sound recordings via new distribution mediums. Many of these changes have been disruptive to traditional business models, but there have also been new opportunities fostered by technological developments. The Internet represents a platform for entrepreneurship and expression but at the same time it also has produced tremendous financial difficulty for those in the creative community who earn their living from their copyrights, from recording artists to labels to songwriters to publishers, as well as those who distribute and market and provide support to our community.*
>
> *"Despite the many unresolved questions surrounding the protection of Intellectual Property online, we remain optimistic that open Internet structures are our best means through which to do business for legally distributed content. At the same time rampant Internet piracy has resulted in a reduction in our revenues due to the ease with which Internet users can acquire our musical copyrights from illegal sources around the world without compensating the music creators or those that invest in that creation. One of our greatest opponents are search engines linking to sites that allow access to unlicensed music , as is done by services like Google to sites like RapidShare in Germany (selling their Google ads along the way), with no piracy search engine linking liability. We need our legislators to focus on closing these links which encourage illegal activity."*

ATTACHMENT A

From: Twitter Support [mailto:support@twitter.zendesk.com]
Sent: Friday, November 05, 2010 2:22 PM
To: RIAA Antipiracy
Subject: #1335759 Copyright complaint procedure

Please do not write below this line

Ticket #1335759: Unauthorized sound recordings and Twitter rules violation
<http://twitter.zendesk.com/tickets/1335759>

Hi RIAA Antipiracy,

This auto-response from Twitter contains information regarding your copyright request. We do not accept attachments for security reasons; if you haven't mailed or faxed your information, please reference this ticket number when you do. If you've already faxed your information, there is no need to reply to this email.

Copyright complaints concern the unauthorized distribution or republishing of material protected by copyright law. If you are reporting a copyright violation, you must mail or fax a DMCA take down notice signed by the copyright owner or someone legally authorized to act on their behalf.

Submit DMCA take down notices by mail to:

Twitter Inc.,
c/o Trust and Safety
795 Folsom Street, Suite 600
San Francisco, CA 94107
Fax to: 415-222-0922

Please note that our copyright agent is unable to accept support requests, or requests related to trademark, impersonation, and other Terms of Service violations. Our copyright policy is here:
http://help.twitter.com/forums/26257/entries/15795

----Helpful Hints-----

If your request does not involve an image protected by copyright or links to unauthorized publication of copyright protected materials, chances are, it's not a copyright request. Examples of copyright violations:

1. A Twitter account publishing links to free downloads of copyright protected materials

2. A Twitter account using a copyright protected logo or image (please ensure that the image is not protected by fair use before submitting a take down notice.)

Many people confuse copyright with trademark. A trademark complaint is not a copyright complaint; trademark and/or other Terms of Service requests should be sent to our Terms of Service team by filing a web request here:
http://twitter.zendesk.com/requests/new

Or, if you don't have a Twitter account, send your complaint to:
terms@twitter.com

Our trademark policy is here:
http://help.twitter.com/forums/26257/entries/18367

Thanks,
Twitter Support

This email is a service from Twitter Support

APPENDIX III

ONLINE THEFT FACT SHEET




ONLINE THEFT — THE IMPACT ON FILM, TELEVISION, AND MUSIC INDUSTRY CREATORS, PERFORMERS, AND CRAFTSPEOPLE – AUGUST 2010

AFTRA, DGA, IATSE, and SAG represent over 300,000 workers who create a multitude of diverse films, television programs, and sound recordings that are sought-after by consumers around the world. Protection of their ability to earn a living from the sale and distribution of that content is the major priority of AFTRA, DGA, IATSE, and SAG.

- The motion picture and television business relies heavily on "downstream" revenue from the exploitation of our product in secondary markets, after initial distribution on television or in a movie theatre.
    - These revenue sources not only drive investment in the motion picture and television industry, but they directly fund our members' residual compensation and pension and healthcare plans.
    - Never was this reliance on downstream revenue more significant than it is today — 75% of a motion picture's revenues come from markets after the initial theatrical release, and more than 50% of scripted television revenues are generated after the first run.
- The music industry has sustained itself for decades on the fundamental model of investment in and the sale of sound recordings.
    - The Internet has become a vital sales and distribution platform for music, but online theft of sound recordings has made it increasingly difficult for recording artists to earn a living.
    - Unlawful downloading, file sharing, and digital theft constitute a direct attack on the legitimate sale and distribution of copyrighted material upon which recording artists and background vocalists rely.
- Currently, downstream revenues from the reuse of feature films and television programs and lawful sales of sound recordings generate $1.4 billion annually in essential residuals and royalties for our members. In 2009,
    - For AFTRA recording artists, 90% of income derived from sound recordings was directly linked to royalties from physical CD sales and paid digital downloads;
    - DGA members derived 19% of their compensation from residual payments;[1] and
    - SAG members who worked under the feature film and television contract derived 45% of their compensation from residuals.[2]
- Residuals and royalties *also* play a significant role in funding the health and pension plans that benefit all of our members. These benefits provide a guaranteed safety net for our members, and are part of our industry's long-established and collectively bargained agreements.
- In 2009, residuals derived from the sale of Features to Free TV and/or Features and Free TV to supplemental markets (Pay TV, DVD, viewing on airplanes, etc.) funded:
    - a 71% of DGA's Basic Pension Plan;
    - a 65% of the MPI Health Plan (for IATSE Members); and
    - a 31% of SAG's Pension and Health Plan.

[1] Residual payments also fund most of the Basic Pension Plan.

[2] Reported initial compensation earnings are subject to caps.