

**Comments of Public Knowledge, the Electronic Frontier Foundation, and the
New America Foundation
in the Department of Commerce's Internet Task Force
Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy**

*Docket No. 100910448-0448-01
RIN 0660-XA19*

November 19, 2010

Table of Contents

INTRODUCTION 1

STREAMING, CYBER LOCKERS, AND FILTERS 2

 CYBER LOCKERS AND STREAMING TECHNOLOGY HAVE LEGITIMATE USES 3

**LITIGATION HAS NOT REDUCED DIGITAL COPYRIGHT INFRINGEMENT AND IS
CAUSING SIGNIFICANT COLLATERAL DAMAGE 5**

**THE U.S. GOVERNMENT’S POWER TO PREVENT ILLEGITIMATE ACTIVITY ONLINE IS
LIMITED BY GEOGRAPHY 8**

**THE GOVERNMENT’S POWER TO PREVENT ILLEGITIMATE ACTIVITY ONLINE IS
LIMITED BY TECHNOLOGY 11**

**VOLUNTARY COLLECTIVE LICENSING: A MODEL FOR ENABLING INNOVATION AND
COMMERCE 13**

INTERMEDIARIES 14

 INTERMEDIARIES ARE GOOD AT MOVING DATA, BAD AT POLICING 15

 LOOK TO CONGRESS FOR GUIDANCE ON BALANCE 15

If Conduits are Required to Police a Little, They Will be Pressured to Police a Lot 22

Policing Requirements Set the Stage for Restrictive Private Agreements 23

 IMPROVEMENTS TO NOTICE AND TAKEDOWN 25

PROTECTING INNOVATION 29

 A LEVEL PLAYING FIELD WILL HELP PROMOTE FUTURE SUCCESSFUL BUSINESS MODELS 30

 THE DEPARTMENT SHOULD BE WARY OF INCUMBENT-GENERATED COMMON STANDARDS 31

CONCLUSION 32

INTRODUCTION

Public Knowledge the Electronic Frontier Foundation, and the New America Foundation (“Commenters”) welcome the Department of Commerce’s review of the relationship between digital copyright and online innovation. In considering the relationship between copyright and innovation, it is critical to remember that copyright is fundamentally a balance between the rights of the creator and the rights of the public at large. It is unavoidable that copyright creates restrictions on free expression and the free flow of ideas. However, it can also provide a powerful incentive to create. Effective copyright policy finds an equilibrium between the creator’s incentive to create and the public’s right to access, share and build on existing works. To that end, the Department should focus on finding ways to encourage more people to create and contribute. In addition to benefits, the costs of enforcement - both financial and in increased barriers to innovate - must be considered.

The best way to encourage creativity and innovation in the Internet economy is to reduce barriers to creativity and innovation. Services like iTunes and Netflix show that copyright infringement is best addressed through innovation, not restrictive rights management schemes or by making it harder for the public to access works. The safe harbor provisions of the Digital Millennium Copyright Act (DMCA) have spurred that kind of innovation. They establish clear procedures through which copyright owners can cause the expeditious removal of allegedly infringing material, empower users to challenge improper removals, and allow service providers to develop new services in a climate of relative legal certainty.

By contrast, aggressive, government backed copyright enforcement efforts can have unintended repercussions. For example, foreign governments can use copyright law as a pretext for suppressing internal dissent. Recent reports of Russian police using allegations of copyright infringement to crack down on civil society groups highlight the realities of such abuse.¹ Here in the U.S., a recent proposal to authorize the Department of Justice to create a “blacklist” of sites allegedly dedicated to infringing activities and encourage ISPs to block such sites has sparked a wave of protest from a variety of groups, from software engineers² (including many who developed the initial architecture of the Internet) who fear the proposal will fundamentally undermine the domain name system, to human rights groups who believe it will send a signal to the world that the United States supports Internet censorship, as long as it is disguised as copyright enforcement.³

We urge the Department to identify and promote copyright policies that recognize the extraordinary public benefits of online innovation and creativity, and seek to ensure that those benefits are not lost in the name of policing infringement.

STREAMING, CYBER LOCKERS, AND FILTERS

The Department noted that some stakeholders expressed concerns that tools such as cyber locker services and streaming were increasingly being used to facilitate

¹ Clifford J. Levy, *Russia Uses Microsoft to Suppress Dissent*, N.Y. Times, Sept. 11, 2010, at A1, available at <http://www.nytimes.com/2010/09/12/world/europe/12raids.html>.

² *An Open Letter From Internet Engineers to the Senate Judiciary Committee*, Sep. 28, 2010, available at <http://www.eff.org/deeplinks/2010/09/open-letter>.

³ Letter from American Civil Liberties Union, *et. al.* to Patrick J. Leahy, Chairman, United States Senate Judiciary Committee and Jeff Sessions, Ranking Member, United States Senate Judiciary Committee (Oct. 26, 2010), available at http://www.eff.org/files/filenode/coica_files/COICA_human_rights_letter.pdf.

copyright infringement.⁴ Cyber lockers and streaming services are tools that are useful for accessing large files from anywhere in an always-connected environment. They are also a convenient way to share large files, like a long report with complex graphical elements that may be too large to transfer by email, between geographically remote individuals. Large groups of people can use a single cyber locker to coordinate projects and synchronize information even if they do not share an office or access to the same network. As file sizes grow larger and Internet connectivity grows increasingly omnipresent, so too will the use of cyber lockers and streaming technology. However, it is certainly possible to use cyber lockers to facilitate copyright infringement. Storing files, just like transferring files, can be used for both legitimate and illegitimate purposes.

When examining tools such as cyber lockers and streaming technology, the Department would be well served to remember that all tools can be used for legitimate and illegitimate purposes. Targeting general-purpose tools used to store and transfer files instead of the specific illicit behavior of concern is an inefficient and disruptive way to achieve a goal. We do not address concerns about mail fraud by shutting down the postal service.

Cyber Lockers and Streaming Technology Have Legitimate Uses

The legitimate uses of cyber lockers and streaming technologies are many and varied. Cyber lockers are a quick and easy way to share files with large numbers of people. For example, before Public Knowledge releases a video to the public, it is often useful to share and edit the video internally. Due to the limits of the Public Knowledge

⁴ Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy, Docket No. 100910448-0448-01, *Notice of Inquiry*, 75 Fed. Reg. 61422 (Oct. 5, 2010) (“NOI”).

email system (both in the size of email attachments and in inbox capacity), it is often much easier to upload the video to a cyber locker and simply distribute the corresponding URL to interested staff members.

Cyber lockers such as DropBox or Ubuntu One allow users to safely and efficiently upload, backup, and synchronize their files (be they contacts, bookmarks, documents, or music) to the cloud, giving them the ability to access their files from anywhere and share those files as necessary. The much discussed “cloud computing,” promoted by companies such as Microsoft, Cisco, and Amazon, rely on technologies like cyber lockers and streaming technology to make their offerings viable. The General Services Administration recently embraced cloud computing for the Federal Government when it launched Apps.gov. The ever-decreasing cost of Internet connectivity and digital storage make these always-on, always-available services low cost solutions for many consumers, businesses, and governments.

Streaming technology gives consumers and creators the ability to quickly and easily share all types of media without requiring bulky downloads. Once they are finalized internally, those same Public Knowledge videos are streamed to the public via sites such as YouTube. The list of industries, content providers (both large and small), distributors, creators, and even hardware manufacturers that have embraced streaming media would fill many pages of comments. In fact, some reports suggest that streaming is rapidly becoming the preferred way to access media files.⁵

There is no doubt that, in addition to hundreds of legitimate uses, cyber lockers and streaming can also be used for illegitimate ends. However, the Department cannot

⁵ Eliot Van Buskirk, *Americans Now Stream Music As Often As They Download*, Evolver.fm, Nov. 11, 2010, available at <http://evolver.fm/2010/11/11/americans-now-stream-as-much-music-as-they-download/>.

allow the fact that a tool can be misused to cause it to overlook the myriad benefits that these tools provide. Instead, it should look to the wisdom of Congress including section 512(a) in the DMCA⁶ and section 230 of the Communications Decency Act,⁷ provisions that allow intermediaries to facilitate communication without living in fear of massive liability. Similarly, it should note the example set by the Supreme Court in *Sony Corp. v. Universal City Studios*, when the Court refused to sacrifice the substantial noninfringing uses of the VCR merely because it was a tool that could also be used for copyright infringement.⁸ Simply because it is possible to use the Internet for illicit purposes should not lead us to declare it off limits.

LITIGATION HAS NOT REDUCED DIGITAL COPYRIGHT INFRINGEMENT AND IS CAUSING SIGNIFICANT COLLATERAL DAMAGE

The Department asked about the efficacy of litigation in preventing online copyright infringement.⁹ As an empirical matter, more than seven years of high-profile lawsuit campaigns by rightsholders have had little measurable effect on online copyright infringement. For example, at the height of the Recording Industry of America's (RIAA) litigation campaign in 2007 and 2008, various file-sharing venues reported stratospheric growth in visitors, searches, and software downloads.¹⁰

⁶ Codified at 17 U.S.C. § 512.

⁷ Codified at 47 U.S.C. § 230.

⁸ *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 422 (1984).

⁹ *NOI* at 61422.

¹⁰ Janko Roettgers, *Limewire Wants to Give Record Labels a Cut of Its Ad Revenue*, P2P Blog, May 13, 2008, (noting LimeWire has 80 million users generating about 5 billion search requests every month, putting Limewire on par with search engine giants like Google and Yahoo); Posting of Ernesto to TorrentFreak, *BitTorrent Trio Hit a Billion Pageviews a Month*, (June 11, 2008) (describing three BitTorrent websites—Mininova, The Pirate Bay, and isoHunt—that have entered the list of top 100 most visited websites on the Internet); BNET Business Wire, *Azureus Announces One Million Unique Visitors to Its Digital Media Platform Currently Code Named Zudeo*, February 16, 2007, (boasting that

Moreover, in the past year the mass litigation strategy pioneered by the RIAA – a strategy the RIAA has wisely abandoned – has unfortunately spawned copycat lawsuits from law firms leveraging the statutory penalties in copyright law to secure settlements from alleged downloaders, with little regard for the individual's due process rights. In the past year alone, over 55,000 people have been sued as “John Does” for allegedly downloading and/or uploading copyrighted material.¹¹ For example, a Washington, D.C., law firm calling itself the U.S. Copyright Group (USCG), that has filed several “John Doe” lawsuits in D.C., implicating over 14,000 individuals. Righthaven LLC, has brought over 130 lawsuits in Nevada federal court claiming copyright infringement. Righthaven scours the Internet for newspaper stories (or parts thereof) originating with the Las Vegas Review-Journal that have been posted on blogs, forums and webpages, acquires the copyright to that particular newspaper story, and then sues the poster for copyright infringement.¹² Righthaven demands sums up to \$150,000, and uses the threat of these disproportionate damages to push defendants into quick settlements, even where they have legitimate fair use or other defenses. Finally, cases have recently been brought by adult entertainment companies, targeting over 40,000 people as of November 8.¹³ After suing the users as “Does,” based on their IP addresses, the companies promptly subpoena the identities of people associated with those IP addresses. Unfortunately, many of those people, who are not comfortable being publicly identified in connection with

Azureus is "the provider of the most popular P2P application for the transfer of large files" and citing over 140 million downloads of its application in the past few years).

¹¹ Corynne McSherry, *A Field Guide to Copyright Trolls*, Sept. 28, 2010, available at <https://www.eff.org/deeplinks/2010/09/field-guide-copyright-trolls>.

¹² *Id.*

¹³ Violet Blue, *Every Inch Counts: Porn Filesharing Lawsuits Crest 30K Defendants*, ZD Net, Nov. 8, 2010, available at <http://www.zdnet.com/blog/perlow/every-inch-counts-porn-filesharing-lawsuits-crest-30k-defendants/14509>.

pornography, will feel they have no choice but to settle rather than having their name publicly disclosed, no matter how meritorious their defenses.

These lawsuits depend on the success of two strategies. First, cookie-cutter litigation tactics, such as filing one lawsuit against thousands of legally unrelated people in a court convenient to the lawyers, even if it means the targets will have to defend themselves thousands of miles from home. Second, targeting vulnerable defendants, who will be eager to settle even if they have strong defenses. This eagerness is because they cannot afford the risk of an award of substantial damages if the case went to trial, are unable to obtain counsel far from home, or are afraid of the consequences of having their personal information made public (e.g., the defendants targeted in the adult entertainment cases).

The rapid evolution of technology for storing and distributing large files on the Internet shows that entrepreneurs and innovators are responding to consumer and business demand for file storage and distribution services that are efficient, flexible, easy to use, and stable – like a "corporate intranet" for Internet users at large. Litigation over these sites and services carries with it the risk of stifling the growth of these services and the mainstream benefits that they provide. And mass litigation against individual users risks enormous collateral damage to both our traditional notions of due process and the many individuals who have meritorious defenses but must nonetheless settle their case because they cannot afford not to.

THE U.S. GOVERNMENT'S POWER TO PREVENT ILLEGITIMATE ACTIVITY ONLINE IS LIMITED BY GEOGRAPHY

While the government's goal of enforcing its laws and protecting rightsholders may be a laudable one, it must account for limitations to its own power. The Internet is a global network that extends well beyond our national borders, and websites operating outside of the jurisdiction of the United States are often just as accessible as those operating next door.¹⁴ As a result, the ability of any individual government to punish bad actors online is limited and imperfect. However, attempting to overcome these limits through novel jurisdictional hooks can create newer, potentially more serious problems.

Although cyber lockers and streaming sites can be accessed from the United States, they are not necessarily hosted in the United States. The organizations responsible for the sites may not have any formal contacts with the United States or have assets in the United States. Many are not even targeted at users in the United States. This limits the United States' ability to enforce its law against them.

These limitations are important because they work both ways, preventing foreign governments from imposing unwanted rules on our own domestic entities. When France demanded that Yahoo! remove Nazi-related material that violated French law, U.S. courts refused to enforce the order because it conflicted with our First Amendment.¹⁵ Similarly, countries like Iran are unable to regulate the activities of U.S. Internet companies simply because it is possible to access those sites from Iran.

¹⁴ As the Department noted, overseas sites can be the source of some infringing materials. *See NOI* at 61422.

¹⁵ Troy Wolverton, *Court Shields Yahoo from French Laws*, CNET News.com, November 8, 2001, available at <http://news.cnet.com/2100-1017-275564.html>.

Recently, there have been attempts to single out pieces of the Internet architecture that are located domestically and use those as levers to exert control over elements of the Internet outside of the United States.¹⁶ As noted above, the most recent attempt, the Combating Online Infringement and Counterfeits Act (COICA), has been poorly received because its provisions are ill-conceived and threaten the fundamental underpinnings of the Internet.¹⁷

In attempting to achieve the narrow policy goal of fighting online infringement and counterfeiting, COICA would effectively fracture the Internet. It tried to address problems that are international in scope by singling out important elements of the Internet that happen to have a connection to the United States.

COICA targets enforcement actions against domain registration companies operating out of the United States and top-level domains like .com and .org that are based in the United States. It also targets the Domain Name Server (DNS) system – an attractive target because many DNS servers happen to be located in the United States and operated by domestic corporations – the provisions would undermine the unified system for matching website names with actual website addresses. COICA encourages the creation of multiple, unconnected DNS servers instead of a simple, accessible, and universal DNS system.

COICA also sets a dangerous precedent undermining due process. It encourages the Justice Department to maintain a public blacklist of websites that the Justice Department unilaterally determined “upon information and reasonable belief” to be

¹⁶ Combating Online Infringement and Counterfeits Act, S.3804, 111th Cong. (2010) (COICA)

¹⁷ Sherwin Siy, *New Copyright Bill Bears Problems: Concerns with 2.3804, the Combating Online Infringement and Counterfeits Act (COICA)*, September 25, 2010 available at <http://www.publicknowledge.org/blog/new-copyright-bill-bears-problems-concerns-s3>.

dedicated to infringing activities. Once on this blacklist, which would operate with limited judicial review, sites would be hard to access through most commercial Internet Service Providers (ISPs).

It is not hard to imagine how this process could be abused. Copyright infringement notices of questionable validity are already regularly used to suppress political speech.¹⁸ Magnifying those (often groundless) accusations by adding accused content to a government blacklist further increases the disruptive impact of a well-timed but poorly-grounded accusation. Furthermore, a process of blacklisting websites simply “upon information and reasonable belief” could set a dangerous precedent for regimes looking to legitimize their own online censorship.

Alternative language being discussed for inclusion in COICA would replace a government blacklist, and instead absolve critical intermediaries (such as domain name registrars or financial transaction providers) from “voluntarily” blocking access to sites. By removing the threat of legal liability for disrupting the free flow of information online, but not mitigating the threat of secondary liability for allegedly contributing to copyright infringement, this provision exposes intermediaries to extreme pressure by large rightsholders to massively disrupt the Internet.

Of course, COICA is but the latest example of this approach to addressing concerns of rightsholders. Moving forward, the Department must be wary of any suggestions to overhaul the design of the Internet in order to achieve narrow policy goals. Weakening a critical communications platform in the hopes of curbing a specific type of activity will inevitably result in unexpected and wide ranging consequences.

¹⁸ Center for Democracy and Technology, *Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech*, September 2010 available at http://www.cdt.org/files/pdfs/copyright_takedowns.pdf.

THE GOVERNMENT’S POWER TO PREVENT ILLEGITIMATE ACTIVITY ONLINE IS LIMITED BY TECHNOLOGY

The Department inquired into the status and effectiveness of technologies used to detect or prevent online infringement.¹⁹ These technologies have proven to be both ineffective at combating online infringement and disruptive of legitimate activities. Even if the Department were somehow able to impose technological solutions across the entire Internet to reduce copyright infringement, those solutions would inevitably be flawed. Technological solutions to complex problems will more often than not create unintentional harms, be subject to unforeseen weaknesses, and in the meantime be defeated by effective countermeasures.

First and foremost, many solutions designed to reduce copyright infringement implicate significant privacy concerns. In order to determine if transmitted data is infringing, a filter must first determine what the transmitted data is. In the absence of a machine readable flag identifying the content, any automated system would need to examine the content being transmitted. Because there is no way of knowing which unknown packets are infringing and which unknown packets are noninfringing, any filter must carefully examine *all* packets. Tim Berners-Lee, widely credited as the creator of the World Wide Web, denounced deep packet inspection (DPI) – the technology used to examine the contents of packets on a network – as the digital equivalent of opening another’s mail, putting a camera in a private room, or wiretapping.²⁰ DPI is

¹⁹ *NOI* at 61422.

²⁰ Barry Collins, *Berners-Lee: Phorm is like a “TV camera in your room,”* PCPro, March 11, 2009 available at <http://www.pcpro.co.uk/news/249374/berners-lee-phorm-is-like-a-tv-camera-in-your-room>.

simultaneously incredibly invasive to average users and easily circumvented by motivated parties through encryption and other obfuscation techniques.

Digital watermarking can be used to help identify content when that content is being displayed or performed publicly, removing the need for privacy-invasive DPI. Unfortunately, watermarking does nothing to solve a more fundamental problem of automated copyright systems—it cannot be used to effectively identify the *uses* of that content. Therefore, even if a technology can identify the content, it is unlikely that it will be able to effectively determine if the use violates copyright law.

There simply is not a technological filter capable of effectively separating infringing from non-infringing uses.²¹ For example, one major question in determining whether an online use of a work is infringing is whether it is a fair use. Making that determination requires a complex, multi-factor test that even judges have trouble applying consistently. Any automated filter will inevitably over-block legitimate uses of copyright-protected works.

Other legal and legitimate uses may also be over-blocked by automated filters. One ready example is uses that have been permitted by the copyright holder. Copyright permissions do not travel with files. A copyright owner who had submitted a song for filter inclusion could, much later, attempt to send the file to a friend or colleague. The filter would block the transfer simply because the song matched a “block” list. The filter would have no reliable way of knowing that the transfer was authorized by the rightsholder.

²¹ For more detail on the various problems with technological filtering of copyright, see Mehan Jayasaira, *et. al. Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Viable Solution for U.S. ISPs*, July 2009 available at <http://www.publicknowledge.org/pdf/pk-filtering-whitepaper-200907.pdf>.

Third, attempts to address these shortcomings move increasingly towards heavy-handed censorship. Easy to implement systems with bright line rules can appear to be attractive solutions. However, if systems that do not respect the legal nuances surrounding free speech and the balances inherent in copyright law are widely adopted, they become *de facto* law. This *de facto* law would exclude precisely the type of marginal expression that it is most important to protect.

Finally, history shows that any technological attempt to reduce copyright infringement will be circumvented. Parties interested in infringing copyrighted works will continue to do so. Given enough time, they will find a way to circumvent even the most elegantly designed DRM or filtering system. As a result, any given technological attempt to prevent illegitimate copying will fail, and may even exacerbate matters by spurring the growth of *private or encrypted networks where traffic is less easily monitored*.²² Thus, the primary lasting impact of technological protection measures is increased inconvenience for the public while reducing freedom of expression.

VOLUNTARY COLLECTIVE LICENSING: A MODEL FOR ENABLING INNOVATION AND COMMERCE

The Department should consider promoting alternative models for cooperation, such as collective licensing. In the first half of the 20th century, copyright-bearing songwriters viewed the burgeoning broadcast radio industry as "pirates," much like today's copyright-bearing music and film companies view peer-to-peer file sharing and

²² See Peter Biddle, *et. al.*, *The Darknet and the Future of Content Distribution*, (Microsoft Corp. 2002) available at <http://msl1.mit.edu/ESD10/docs/darknet5.pdf>.

other digital technologies. Eventually, songwriters came together of their own volition and formed collecting societies like ASCAP, BMI and SESAC. These voluntary collecting societies offered radio stations the right to play whatever music they wanted in return for a fee, which the collecting society then distributed to member songwriters.

The voluntary collective licensing scheme for radio opened the doors for dramatic growth and innovation while simultaneously granting songwriters a way to harness the disruptive innovation of wireless audio transmission. Today, the performing-rights societies ASCAP and BMI still collect money and pay out millions annually to their artists. This historical example of voluntary collective licensing offers a glimpse of what measures – voluntarily undertaken by copyright owners – could work to promote innovation and stimulate economic activity around copyrighted works. Thus, we urge the Department to sponsor meetings among stakeholders to discuss how a collective licensing system can be accomplished.

INTERMEDIARIES

The Department is wise to focus on experiences with intermediary liability.²³ The potential sources of infringing content are relatively numerous and far-flung. However, the paths that those sources travel are relatively few and geographically concentrated. As a result, there is often an impulse to involve intermediaries in attempts to reduce copyright infringement. Unfortunately, this impulse can lead to a host of negative consequences.

²³ *NOI* at 61422-23.

Intermediaries Are Good at Moving Data, Bad at Policing

Imposing liability on general-purpose communications intermediaries for the information they carry would massively increase the burdens of operating the Internet. Faced with such liability, a communications provider would essentially be forced to choose between two unattractive options: inspect (either manually or electronically) every bit of information passing over the network to guarantee it is not transporting objectionable material, or (more or less selectively) stop transmitting data altogether. Inspection would slow transmission, invade privacy, and have limited effectiveness. Stopping transmission would cripple the usage of online services, or in a worst-case scenario, grind the Internet to a halt.

Furthermore, intermediaries come in all sizes. While some of the largest ISPs might be able to shoulder the financial burden of implementing an inspection regime, they would be the exception. For most intermediaries, including both small providers of Internet access as well as providers of online services, sites, and applications, the cost of such a system, assuming it existed at all, would be prohibitive to implement and maintain.

Look to Congress for Guidance on Balance

When considering how to balance the calls to turn intermediaries into copyright police with the need to keep the Internet free from unnecessary choke points and interference, the Department should look to this example set by Congress. Although imposing wide-ranging liability on conduits and service providers would be destructive to open and timely communications, there are instances where intermediaries and service

providers are the logical place to address concerns related to the transmission of information. Congress balanced these two competing realities in both section 230 of the Communications Decency Act²⁴ and section 512 of Title 17.²⁵ In keeping with the Department's own emphasis in its NOI, we will focus here on the latter provision.

In order to assess how well the safe harbors are working, it is useful to start by recalling what they were designed to accomplish. Congress intended the DMCA to “facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education”²⁶ “[B]y limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.”²⁷ In order to accomplish these goals, Congress created a set of “safe harbors” designed to “provide ‘*greater certainty* to service providers concerning their legal exposure for infringements that may occur in the course of their activities.’”²⁸ Congress focused on creating a more predictable legal environment because it recognized that:

[W]ithout clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability. For example, service providers must make innumerable electronic copies by simply transmitting information over the Internet. Certain electronic copies are made to speed up the delivery of information to users. Other electronic copies are made in order to host

²⁴ Codified at 47 U.S.C. 230.

²⁵ Codified at 17 U.S.C. 512.

²⁶ S. REP. NO. 105-190, at 1-2 (1998). Much of the DMCA's legislative history has been compiled by the Home Recording Rights Coalition at <http://hrrc.org/index.php?id=20&subid=3> (last visited July 21, 2010).

²⁷ *Id.* at 8.

²⁸ *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (quoting S. REP. NO. 105-190, at 20 (1998)) (emphasis added).

World Wide Web sites. Many service providers engage in directing users to sites in response to inquiries by users or they volunteer sites that users may find attractive. Some of these sites might contain infringing material. In short, by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.²⁹

Thus, Congress correctly understood that the application of ambiguous copyright doctrines to new Internet technologies would put service providers in an impossible position. Service providers necessarily must make, manipulate, and transmit multiple copies of content at several stages of their technical processes. These multiple copies might arguably infringe one or more of the display, performance, distribution, reproduction, or other rights in copyrighted content. During the Senate hearings preceding the DMCA, Roy Neel, President and Chief Executive of the United States Telecom Association stated the problem as follows:

We have no way of knowing what those trillions of bits of information are flowing over our networks. We simply cannot do it, and to be held liable for those transmissions is simply nonsense and it will tie us up in court, create more litigation and more work for lawyers, but won't do anything to advance the construction and deployment of the Internet, nor will it protect copyright owners to any significant degree.³⁰

In fact, by the time Congress took up the issue in 1997, online service providers had already been embroiled in copyright litigation over the activities of their users.³¹ Thus,

²⁹ S. REP. NO. 105-190, at 8.

³⁰ Copyright Infringement Liability of Online and Internet Service Providers: Hearing Before the Committee on the Judiciary United States Senate on S. 1146, 105th Cong. 29 (1997) (Transcripts of the Sept. 4, 1997 hearings are available at: <http://www.eric.ed.gov/ERICWebPortal/recordDetail?accno=ED418703>); see also S. REP. NO. 105-190, at 30.

³¹ See, e.g., Jeffrey R. Kuester & Daniel R. McClure, *SPA v. ISPs: Contributory Copyright Infringement in Cyberspace*, INTELLECTUAL PROPERTY TODAY, Feb. 1997, at 8 (describing lawsuits by the Software Publishers Ass'n against online service providers).

Congress enacted safe harbors for secondary liability that were “absolutely necessary to the immediate survival of ISPs.”³²

In return, copyright owners were given several new remedies against infringers. The first of these is an expedited, extrajudicial “notice-and-takedown” procedure for obtaining redress against alleged infringement.³³ Second, copyright owners were given the power to issue pre-complaint subpoenas to service providers like Veoh in order to identify and locate infringing Internet users.³⁴

One of Congress’s principal motivations for establishing clear rules regarding intermediary liability for the acts of users was to foster the development of the Internet as a platform for free expression. In the words of Rep. Barney Frank:

One of the things we do here is to say: “If you are an on-line service provider, if you are responsible for the production of all of this out to the public, you will not be held automatically responsible if someone misuses the electronic airway you provide to steal other people’s property.”

. . . .

We have hit a balance which fully protects intellectual property, which is essential to the creative life of America, to the quality of our life, because if we do not protect the creators, there will be less creation. But at the same time we have done this in a way that will not give to the people in the business of running the online service entities and running Internet, it will not give them either an incentive or an excuse to censor.³⁵

Thus, with § 512, Congress enacted special copyright rules for service providers that might otherwise be held liable for the actions of their users.

³² *CoStar Group Inc. v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004), *aff’d*, 373 F.3d 544 (4th Cir. 2004).

³³ § 512(c)(1)(C).

³⁴ § 512(h).

³⁵ 144 CONG. REC. H7092 (daily ed. Aug. 4, 1998) (floor statement of Rep. Barney Frank) *available at* <http://hrrc.org/File/2281HouseDebateAug4.pdf>; *see also* 144 CONG. REC. H10618 (daily ed. Oct. 12, 1998), *available at* <http://hrrc.org/File/HR2281StearnsOct12.pdf>.

Those rules have been wildly successful at accomplishing Congress's purpose. In the twelve years since Congress enacted the DMCA, the Internet has revolutionized the creation and dissemination of speech. With the help of online service providers like Wikipedia, the Internet Archive, Google, YouTube, Blogger, Twitter, Facebook, MySpace, Flickr, and many others, individuals with little technical knowledge or money can today find, create, reproduce, disseminate, and respond to content, interacting with a global audience. Interactive platforms like video hosting services, bulletin boards, and social networking sites have become vital to democratic participation and the ability of Internet users to forge communities, access information, and discuss issues of public and private concern.

Without the predictability provided by § 512, however, the Internet would be a much less hospitable place for free expression and creativity. First, if an intermediary faces the possibility of potentially unlimited legal liability for content hosted, transmitted, or disseminated through its services by a small minority of users, it will feel compelled to scrutinize and limit all user activities. This is likely to lead to over-blocking, sacrificing lawful content in an effort to limit potential litigation.

The strong incentive to over-block can cause particular harm to free speech where, as is often the case, intermediaries are not able to easily determine if the content is unlawful on its face.³⁶ Because the cost to intermediaries to investigate each allegation of infringement will almost always be greater than the cost of simply removing the content, intermediaries have little financial incentive to challenge removal demands. This, in turn,

³⁶ See generally M. Nimmer & D. Nimmer, *Copyright* § 12B.04[A][1] (2005).

will encourage abuse on the part of the governments or private litigants seeking to take down materials for censorial, rather than infringement, reasons.³⁷

Second, if intermediaries face potentially huge legal liability for the unlawful activities of a tiny minority of users, they may simply decide that it is impossible to offer some online services, even where those services are used predominantly for lawful purposes. For example, users post more than thirty-five hours of video to YouTube *every minute*, the vast majority of which are noninfringing and perfectly lawful.³⁸ If liability concerns arising from a minority of these videos compelled a service provider like YouTube or Veoh to pre-approve all user contributions, the service simply could not continue to operate as an open forum for user expression. The same is true of the countless online forums and blogs where users post hundreds or thousands of comments every hour. In the absence of the DMCA safe harbors, fear of liability would likely lead service providers to adopt the same “clearance culture” that characterizes “traditional” television, radio, and other mass media outlets—where even entirely law-abiding creators cannot find an audience without first running a gauntlet of lawyers and insurers.

In addition, service providers have strong market incentives to voluntarily develop better technologies to detect and prevent copyright infringements on their web sites. While the § 512 safe harbors provide an important baseline of legal protections and “rules of the road” for fledgling service providers, they do not give service providers consistent access to big-budget entertainment content. Accordingly, online service

³⁷ See, e.g., *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1204 (N.D. Cal. 2004) (“[n]o reasonable copyright holder could have believed that the portions of the email archive discussing possible technical problems with Diebold’s voting machines were protected by copyright . . . Diebold knew—and indeed it specifically intended—that its letters . . . would result in prevention of publication of that content.”).

³⁸ See *Viacom Int’l, Inc. v. YouTube Inc.*, Nos. 07-2103, 07-3592, 2010 WL 2532404, at *3 (S.D.N.Y. June 23, 2010).

providers have significant business incentives to police for copyright infringement as part of voluntary commercial arrangements with major content owners. For example, the industry leader in online video hosting, YouTube, has been a pioneer in developing and implementing infringement detection tools.³⁹ Other services have enacted similar programs.⁴⁰

Section 512(c) has been crucial to enabling these voluntary efforts between copyright owners and service providers. Because Congress made it clear in § 512(m) that service providers have no legal obligation to monitor their services, service providers have been free to experiment with content identification and monitoring tools without fear that such experimentation might lead to secondary liability. In fact, this measured approach is only possible because § 512(m) relieves service providers from having to embrace simultaneously every tool proposed by every copyright owner.⁴¹ Section 512(m) is even more important when viewed in the context of small or startup intermediaries. A one-size-fits-all solution that assumed all intermediaries had resources on par with YouTube would effectively eliminate all but the largest players.

In certain specific cases, of course, the safe harbors may not apply, and intermediaries can be held liable for information transmitted or required to block the transmission of information. However, parties hoping to overcome that assumption and hold intermediaries liable must meet relatively stringent requirements designed to limit

³⁹ See Rob Hof, *YouTube Intros Video I.D. System; Will Studios Go Along?*, BUSINESS WEEK, Oct. 15, 2007, available at http://www.businessweek.com/the_thread/techbeat/archives/2007/10/youtube_intros.html.

⁴⁰ See *Veoh*, 665 F. Supp. 2d at 1111-1112 (describing voluntary use of Audible Magic fingerprinting technology); *Io Group, Inc. v. Veoh Network, Inc.*, 586 F. Supp. 2d 1132, 1143 (N.D. Cal. 2008) (describing voluntarily implemented “hash,” or digital “fingerprint,” technology).

⁴¹ See BILL ROSENBLATT, GIANT STEPS, CONTENT IDENTIFICATION TECHNOLOGIES 4-7 (2008) (comparing myriad filtering technologies available), available at <http://www.giantstepsmts.com/Content%20ID%20Whitepaper.pdf>.

such actions. More importantly, the intermediary itself is never put in the position of judging claims – it simply complies with properly formed requests from both sides and ultimately defers to judicial decree.

If Conduits are Required to Police a Little, They Will be Pressured to Police a Lot

Currently, intermediaries are not required to police copyright infringement. As explained above, some service providers may follow the notice-and-takedown regime created in §512,⁴² but even then the role of identifying and policing infringement falls primarily to rightsholders and ultimately the courts.

If intermediaries were required to begin peeking deep into packets for possible copyright infringement, there will be calls for them to begin peeking deep into packets for other reasons. In addition to the technological and financial burden this would impose, it would also burden free speech. If every bit of data sent over the Internet is subject to extensive inspection by conduits, sensitive speech will be forced onto alternative channels. This will reduce the value of the Internet as a communications medium and harm freedom of speech.

Beyond copyright, government support for conduits acting as police can negatively impact freedom worldwide. Although the United States might limit support for conduit policing to its own priorities (in this case copyright enforcement), repressive regimes could use that support as a context to use conduit policing for their own particular enforcement priorities. While digitally repressive regimes such as China and Iran are not waiting for an excuse to reduce freedom on their own domestic networks,

⁴² § 512(c).

countries flirting with increased Internet censorship (like those on Reporters Without Borders' *Countries Under Surveillance* list such as Australia, South Korea, and Turkey⁴³) may see conduit policing in the United States as an indication that their own conduit policing programs are within global norms. For example, South Korea requires access providers to filter sites that promote the regime in North Korea.⁴⁴

Policing Requirements Set the Stage for Restrictive Private Agreements

Large content owners do not need government permission to push conduits towards a copyright policing role. Industry organizations such as the RIAA have already attempted to pressure large ISPs into adopting “voluntary” three strikes programs.⁴⁵ Government endorsement of these programs would add to that pressure and allow these agreements to become even more restrictive.

Voluntary agreements between large content holders and intermediaries can be problematic because they only balance the needs of content owners and intermediaries. They lack an inherent incentive to consider the needs of consumers and the public at large. These privately negotiated deals will generally err on the side of over-protection and over-blocking. The costs of over-blocking, high for the public but relatively low for content owners and ISPs, are simply not considered in private negotiations.

Private agreements are not only negotiated in private, but may also remain private after they are finalized. As a result, they suffer from a lack of transparency. Users and

⁴³ Reporters Without Borders *Enemies of the Internet/Countries Under Surveillance* March 2010 available at http://www.rsf.org/IMG/pdf/Internet_enemies.pdf.

⁴⁴ *Id.* at 52.

⁴⁵ David Kravets *Top Internet Providers Cool to RIAA 3-Strikes Plan*, Wired Threat Level, January 5, 2009 available at <http://www.wired.com/threatlevel/2009/01/draft-verizon-o/>.

the general public can be unaware of what, exactly, the parties have agreed to, or how those agreements are implemented in practice.

Copyright-related litigation, like all complex litigation, is time-consuming and expensive. Furthermore, large statutory damages that relieve plaintiffs of the burden of proving actual damages increase pressure for defendants to settle quickly. These costs already create an environment that incentivizes intermediaries to be overly deferential to rightsholders. Adding additional governmental pressure to enter into private agreements would be a disservice to both intermediaries and the public.

At the NTIA listening sessions, several speakers nonetheless suggested that stakeholders could collaborate, voluntarily, to develop standards to help limit online copyright infringement. As an example, they pointed to the UGC Principles,⁴⁶ which have been signed by Microsoft, Disney, DailyMotion and several others. While such collaboration may be helpful in identifying and sharing practices for addressing infringement, it will only truly serve the public if steps are taken to ensure that ALL stakeholders are represented – e.g., users and small service providers as well as media companies and large service providers. Without broad participation, any resulting standards will lack legitimacy and fail to accommodate the spectrum of interests they affect. For example, while the aforementioned UGC principles pay lip service to respecting fair use, signatories did not have to commit to any specific procedures embodying that respect. EFF, Public Knowledge and several other public interest groups have developed an alternative set of UGC Fair Use principles that should assist any future collaboration of this kind.⁴⁷

⁴⁶ NOI at 61423.

⁴⁷ *Fair Use Principles for User Generated Video Content* available at http://www.eff.org/files/UGC_Fair_Use_Best_Practices_0.pdf.

Improvements to Notice And Takedown

After a decade of experience with the DMCA safe harbors, it seems an appropriate time to critically evaluate the effectiveness, volume, and accuracy of notice and takedown regimes.⁴⁸ As discussed, Section 512 provides a formal way for a rightsholder to lodge a complaint, the accused to respond, and for the dispute to move to court for adjudication if necessary.⁴⁹ It also creates safe harbors for service providers and intermediaries. These safe harbors are critical to the creation and growth of new, innovative services.

While notice and takedown is an improvement over intermediaries directly enforcing copyright law, it does suffer from a number of shortcomings. Most strikingly, it perpetuates the power imbalance between large rightsholders and individual users. Users who receive a notice of accused copyright infringement are faced with a stark choice – take down the content in question or claim a legitimate use, potentially provoking a long, expensive trial and massive liability.

Large copyright holders can essentially issue takedown notices in bulk without fear of repercussion: if they are wrong, the accused with either take down the content or submit a counter notice.⁵⁰ If the accused submits a counter notice, the copyright holder has the option to escalate by bringing a formal suit, or simply ignoring the incident and moving on to the next potential infringer. Conversely, when the accused submits the

⁴⁸ NOI at 61423.

⁴⁹ See Senate Judiciary Comm., S. Rep. 105-190 (1998) at 49-51; House Commerce Comm., H. Rep. 105-551 Pt 2 (1998) at 59-60.

⁵⁰ Perhaps the most famous example of a strong fair use argument being ignored is the story of Stephanie Lenz's 29 second video of her children running and dancing in her kitchen with Prince's *Let's Go Crazy* playing in the background. In response to a takedown notice from Universal Music Publishing Group, YouTube took the video down. With pro bono legal help, Ms. Lenz submitted a counternotice and then filed a lawsuit against Universal pursuant to Section 512(f). See <http://www.eff.org/cases/lenz-v-universal>.

counternotice, that party does so knowing she may incur the extraordinary expense and risk of copyright litigation. In addition, while senders of takedown notices are often well-versed in copyright law, users are likely to be laypeople who may have difficulty understanding the DMCA process and the claims against them. In addition, some users will decline to file counter-notices – which normally include contact information and are forwarded to the sender of the takedown notice – because they fear extralegal retaliation.

Shortcomings in the existing DMCA notice and takedown scheme also make it hard to document the one-sided nature of the process. Individuals and small parties are not likely to directly participate in proceedings such as this. They will rarely come forward and tell their own stories about DMCA problems and abuses.

One way to remedy this would be to create an authoritative database of takedown notices.⁵¹ This would allow interested third parties (such as Commenters, other public interest groups, and the Department itself) to develop accurate data about how the notice and takedown process actually functions. It would allow everyone, rightsholders, government policymakers, intermediaries, and the public, do consider the real effectiveness of the notice and takedown regime.

In the meantime, the counter-notice process could be improved in at least two ways. First, intermediaries should publicly commit to forwarding takedown notices to the users targeted whenever possible, so that those targets can better understand the allegations against them. Second, intermediaries should accept counter-notices that are submitted semi-anonymously, such as through an agent, as long as they identify a jurisdiction in which the user can be sued. If it chooses to take the matter to court, a

⁵¹ Although Chilling Effects currently provides a useful database of takedown notices, the database consists of voluntary submissions and is therefore limited. See <http://www.chillingeffects.org/>.

sender of a takedown notice can sue the target as a “Doe” and then seek authorization to issue a subpoena for the Doe’s identity.⁵²

In addition, copyright owners should be encouraged to actually use the system wherever possible. For example, copyright owners – such as Perfect 10 and Righthaven LLC – have refused to take advantage of the notice and takedown system, choosing instead to sue immediately (and/or submit inadequate notices and file a lawsuit when the intermediaries do not respond as desired).⁵³ This approach not only subverts the intent of the safe harbors, it deprives intermediaries of a simple opportunity to cure – contrary to normal practice in other areas of law – and often results in an improper waste of judicial resources.

Finally, one of Section 512’s most important protections for user rights – Section 512(f) – is in need of clarification. To help ensure that the takedown procedure was not abused, Congress created with 512(f) a cause of action against those who knowingly materially misrepresent that a given video, song, or document infringes their copyright. There is little question that such protection is needed: Attacks on free speech through Section 512 misuse are well-documented, from a rodeo organization seeking to shut down critics who posted live video of rodeo events to news organizations demanding the takedown of political ads that use short clips of news coverage, to a movie studio using the DMCA to disable access to a brief video clip of the filming of a new movie.⁵⁴

⁵² See e.g., *Dendrite Int’l v. Doe No. 3*, 775 A.2d 756 (N.J.App. 2001); *Highfields Capital Mgmt. v. Doe*, 385 F.Supp.2d 969 (N.D.Cal 2001).

⁵³ See Jon Healey, *Righthaven: Copyright Lawsuits as a Business Model*, Los Angeles Times, Nov. 4, 2010, <http://opinion.latimes.com/opinionla/2010/11/righthaven-copyright-lawsuits-as-a-business-model.html>; Order, July 26, 2010, *Perfect 10 Inc. v. Google, Inc.*, Case No. 2:04-cv-09484-AHM-SH, available at https://www.eff.org/files/filenode/Perfect10_v_Google/P10_v_Google_on_remand.pdf

⁵⁴ See EFF *Takedown Hall of Shame* available at <http://www.eff.org/takedowns>; see also Dennis Yang, *Viacom Still Not Getting It – Files Bogus Takedown And Kills Some Free Transformers Buzz*, Techdirt, May 14, 2010 available at <http://www.techdirt.com/articles/20100513/2001309420.shtml>.

However, Section 512(f) has thus far been less effective at deterrence than Congress hoped. To make Section 512(f) into a more robust shield against takedown abuse the Department should urge Congress to do the following:

(1) Clarify the Knowledge Standard: Section 512(f) states that a party may be held liable for making a “knowing material misrepresentation” that material is infringing. Defendants in section 512(f) cases have argued that they can only be held liable if they have *actual* knowledge of the misrepresentation, citing *Rossi v. MPAA*, 391 F.3d 1000 (9th Cir), in which the Ninth Circuit Court of Appeals held that “the ‘good faith belief’ requirement in § 512(c)(3)(A)(v) encompasses a subjective, rather than objective, standard.” The *Rossi* case did not involve Section 512(f), but some courts have nonetheless applied it in the Section 512(f) context.⁵⁵

Copyright owners have urged courts to read the *Rossi* ruling to endorse what can be termed the “Moron Defense”: so long as the person sending a DMCA takedown subjectively believed the material to be infringing, no matter how mistaken and unreasonable, there can be no 512(f) liability. Such a reading would encourage copyright owners to hire uninformed investigators who know nothing about copyright law so as to avoid having investigators ever form the requisite subjective intent. This perverse outcome would exacerbate the very problem that 512(f) was meant to address. Commenters do not believe this interpretation is accurate, but in the interest of clarifying the matter, the statute should be revised to state explicitly that a party will face liability if it knows or has reason to know that a given use is authorized or otherwise non-infringing.

⁵⁵ *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D.Cal. 2008); *Dudnikov v. MGA Entmt.*, 410 F. Supp. 2d 1010 (D.Colo. 2005).

(2) Clarify Scope of Damages: Section 512(f) states that the target of an improper takedown may recover for “any damages, including costs and attorneys’ fees.” A federal court has ruled that this statutory language does not include fees and costs associated with bringing a 512(f) lawsuit, and that litigation costs are governed by Section 505 of the Copyright Act.⁵⁶ This interpretation may deter many takedown victims from bringing suit. Unless they are able to obtain pro bono representation, they risk having to pay thousands or possibly hundreds of thousands of dollars in attorneys’ fees. Relatively few users will be willing to take that risk. This interpretation may also discourage attorneys from bringing 512(f) cases, as it makes it more difficult to take such cases on a contingency fee basis, insofar as a prevailing plaintiff has no certainty of recovering attorneys’ fees and costs. Commenters do not believe this interpretation is accurate, but in the interest of clarifying the matter, the statute should be revised to state explicitly that recoverable damages includes costs and fees incurred by the target of a 512(f) takedown in connection with litigation undertaken under Section 512(f).

PROTECTING INNOVATION

The Department rightly focuses on ways to “promote successful, legitimate business models.”⁵⁷ When thinking through the best ways to spur innovation, it is critical to remember that the Internet’s most successful business model has not yet been invented.

⁵⁶ *Lenz v. Universal*, 2010 WL 702466 (N.D.Cal. Feb. 25, 2010).

⁵⁷ NOI at 61422.

A Level Playing Field Will Help Promote Future Successful Business Models

The next great media distribution model will likely not grow from today's large rightsholders. Book publishers did not foster radio broadcasters. Radio broadcasters did not foster movie studios. Movie studios did not foster television networks.

Because there is no way of knowing what the next great innovation in creativity will be, the role of government must be to protect the ability of innovators to enter the market and compete with incumbent services. The most effective way to do that is to maintain the Internet as a level playing field. Like never before, the Internet enables artists and creators to directly connect with fans. A level playing field without gateways fosters the tools and services for this interaction. Preventing online discrimination allows independents to compete against large players on the quality of service offered, not on ability to cut deals with intermediaries.

This makes net neutrality the most important government policy to promoting free expression and the development of new, legitimate business models online. As ISPs look to involve themselves in content creation, and as the existing video distribution operations of many ISPs are challenged by Internet-based upstarts, the motivation to manipulate the flow of information to protect incumbents will only grow. With the dearth of broadband competition all but eliminating competitive pressures to keep the Internet open, only government policies can protect the next great way to legitimately distribute creative content online.

The Department Should be Wary of Incumbent-Generated Common Standards

In the abstract, everyone benefits from common standards and, as the Department recognized, the Internet has certainly benefitted from them.⁵⁸ Common standards drive down prices by making it easier to reach economies of scale, guarantee interoperability across a wide range of devices, and prevent stovepiping with competing and mutually unintelligible standards.

Reality, however, can be less kind to common standards. Without adequate oversight, the creation of common standards by incumbents can become an exercise in anti-competitive behavior. Industry controlled common standards can effectively block new entrants and freeze innovation.

CableCARD, the technology that was originally designed to create a competitive market in video set-top boxes provides a vivid example of industry-driven common standards gone awry. CableLabs, an organization controlled by large cable companies, developed a standard that both prevented all but the most determined independent companies from entering the set-top box market and guaranteed that set-top boxes were not compatible with other subscription video services such as satellite. The standard effectively perpetuated the status quo, forcing the FCC to start from scratch in developing a new standard.⁵⁹

If the Department is interested in developing common industry standards, it must strive to do so in an open, inclusive manner. All parties must rely on an industry-wide

⁵⁸ NOI at 61423.

⁵⁹ See *In the Matter of Video Device Competition*, MB Docket No. 10-91, *Notice of Inquiry*, 24 FCC Rcd. 4275 (2010).

standard (not just new entrants), and licensing terms cannot be used to prevent outside innovators from challenging existing parties or disrupting existing business models.

Ultimately, collaboration between all impacted parties, not collusion by the few, should be the goal. The Department should recognize that independent creators and innovators are often not represented in industry standards setting bodies, and work to ensure that their rights are protected.

CONCLUSION

If copyright policy is focused on locking up existing works and prevent new entrants it will fail at its central purpose: creating the conditions for innovation and expression to blossom. We urge the Department to decline to use its powers solely to explore ways to protect existing business models, and focus instead on balancing the rights and interests of *all* stakeholders so that the Internet can continue to flourish.

 /s/
Michael Weinberg
Sherwin Siy
Public Knowledge

Corynne McSherry
Electronic Frontier Foundation

Tom Glaisyer
Open Technology Initiative
New America Foundation