Comments of the Motion Picture Association of America
Regarding Development of the Joint Strategic Plan
on Intellectual Property Enforcement

Oct. 16, 2015

I. Summary

The Internet has become a tremendous tool for content creators and audiences to connect in innovative and increasingly flexible ways. The legitimate, licensed marketplace for video programming is burgeoning, with more viewers accessing more content through more dissemination channels than ever before. The Motion Picture Association of America's members—Walt Disney Studios Motion Pictures, Paramount Pictures Corp., Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corp., Universal City Studios LLC, and Warner Bros. Entertainment Inc.—have embraced the Internet to offer their content through a wide and growing array of platforms and distributors, and are committed to the continued growth of the online video marketplace.

Unfortunately, the digital era has also taken much of the friction out of piracy. Once an unauthorized copy or stream of content becomes available on the Internet, it is available to the world. Online copyright theft persists, competing with the growth of the legitimate marketplace, stealing revenue, and undermining good U.S. jobs.

We all share an interest in ensuring the Internet continues to develop as a healthy, trustworthy, and safe venue for communication, content, and commerce. Realizing that common goal will require engagement by many public and private sector parties, as well as consumers. At a minimum, reputable companies share a duty not to profit from or facilitate illegal conduct online, including online dissemination of infringing content.

The Internet is, by design, a distributed network that allows anyone around the globe to contribute to and access its content and architecture. This distributed nature, however, also typically means that a user cannot reach particular content or services without the involvement of a large array of intermediaries, including Internet service providers, search engines, advertising networks, payment processors, storage providers, and domain name registries and registrars. The distributed nature also typically means that no single entity can address issues that arise. Solving any given problem will likely require collaboration among a variety of Internet stakeholders.

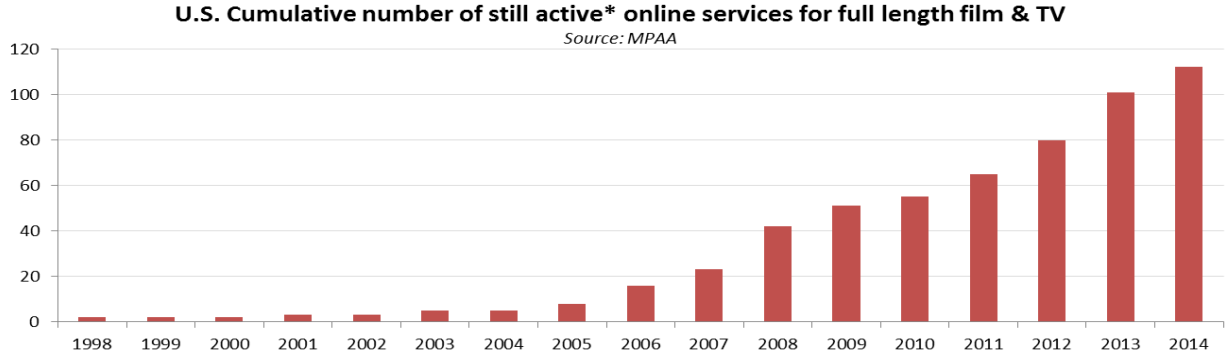
Since the last strategic plan, the Office of the Intellectual Property Enforcement Coordinator has helped get a variety of voluntary initiatives off the ground. They include the Copyright Alert System, a collaboration between ISPs and the content community to inform consumers when their broadband accounts are being used for unlawful peer-to-peer activity and to educate them about lawful online sources of content; efforts by payment processors not to facilitate online transactions in support of copyright infringement; and the Brand Integrity

Program Against Piracy, an initiative to help companies avoid placing advertising on piracy-related web sites. Although the work continues, these represent promising areas of collaboration.

By contrast, at least three areas have shown lagging progress: the use of domain names for unlawful conduct; the prevalence of piracy websites on the first pages of search results; and the use of data storage services to host websites trafficking in stolen content. We ask the IPEC to address each of these issues in the upcoming strategic plan, as well as to continue coordinating enforcement actions against those who engage in pervasive theft of copyrighted content.

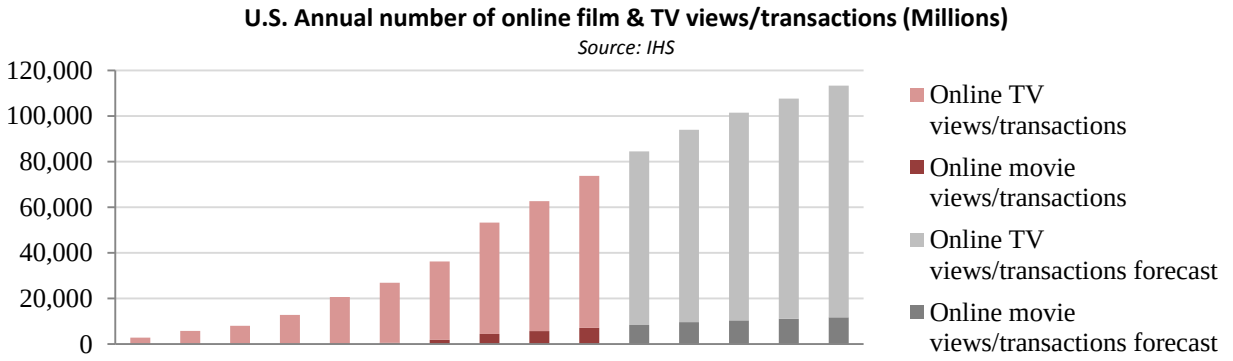
II. Growth in the Legitimate Online Marketplace

Copyright protection under U.S. law continues to drive production and distribution of television programming and films to the public, including over the Internet, by giving creators the exclusive right to determine how their content is disseminated. Recognizing the property right in content creates a marketplace in which creators, distributors, and viewers can enter into a variety of evolving relationships as technology and consumer expectations change. The current market landscape demonstrates the salutary results. In the three years since the MPAA last submitted comments for the Joint Strategic Plan,[1] the number of lawful online sources for television and movie content has almost doubled, and the number of TV episodes and of films that viewers have accessed over those services have almost doubled and quadrupled, respectively. American audiences had access to 112 lawful online video services at the end of 2014, compared to 65 at the end of 2011. They used these services to access 66.6 billion television episodes and 7.1 billion movies in 2014, compared to 34.4 billion television episodes and 1.8 billion films three years earlier, according to IHS data. IHS expects the TV and film numbers to reach 101.6 billion and 11.7 billion by 2019.



1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
2	2	2	3	3	5	5	8	16	23	42	51	55	65	80	101	112

[1] *See* Joint Submission of the Motion Picture Association of America, National Music Publishers' Association, and Recording Industry Association of America (Aug. 10, 2012), *available at* http://www.regulations.gov/#!documentDetail;D=OMB-2012-0004-0248.



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
TV	2,832	5,767	8,025	12,654	20,280	26,325	34,410	48,844	56,921	66,632	74,084	84,320	91,069	96,543	101,561
Films	2	5	22	117	376	577	1,845	4,420	5,727	7,107	8,402	9,650	10,436	11,091	11,739

As the charts above show, the television and movie industry is making far more content available over far more authorized digital services than ever before, including through a variety of business models with diverse price points for broad access. A study by KPMG found that 94 percent of the most popular and critically acclaimed films and between 87 and 96 percent of the most popular and critically acclaimed TV shows were available via online video-on-demand.[2] So while it was never a valid excuse for theft, the claim that video content is not readily available online from lawful sources is also simply not true. The motion picture and television industry has transformed how it does business. Audiences have not been shy about their desire for seamless access to their favorite movies and television shows, at the time and on the device or platform that works best for them, and we have heard them. We are relentlessly innovating to keep meeting that demand, and the choices available to audiences keep growing and diversifying. We welcome and embrace the plethora of new forms of distribution, because they provide us new ways of offering our content to consumers. Of course, business models must present realistic opportunities to recoup investments. But we are in the business of serving consumers, we are attuned to their desires, and we are at the forefront of developing innovative ways to meet those desires.

Indeed, the movie and television industry is making content available online to viewers on every type of in-home and mobile screen, including PCs and Macs, smart TVs, tablets and smartphones, gaming systems, and specialized devices, such as the AppleTV and Roku. Some of this content comes through Internet applications offered by cable and satellite companies. Many content providers also offer programming directly to subscribers through their own authenticated applications, including popular, household-name networks such as A&E, ABC, CBS, CMT, Comedy Central, Disney, ESPN, Fox, Fox Sports, HBO, the History Channel, MTV, NBC, Showtime, Sony, Starz, TBS, TNT, and USA. Content providers also license programming to "over the top" services. And now online distributors are investing in original programming. Netflix, Amazon, and Hulu, for example, are all growing the slate of exclusive content they offer, increasingly involving marquee writers, directors, and actors.

---

2 KPMG, Film and TV Title Availability in the Digital Age (Sept. 2014).

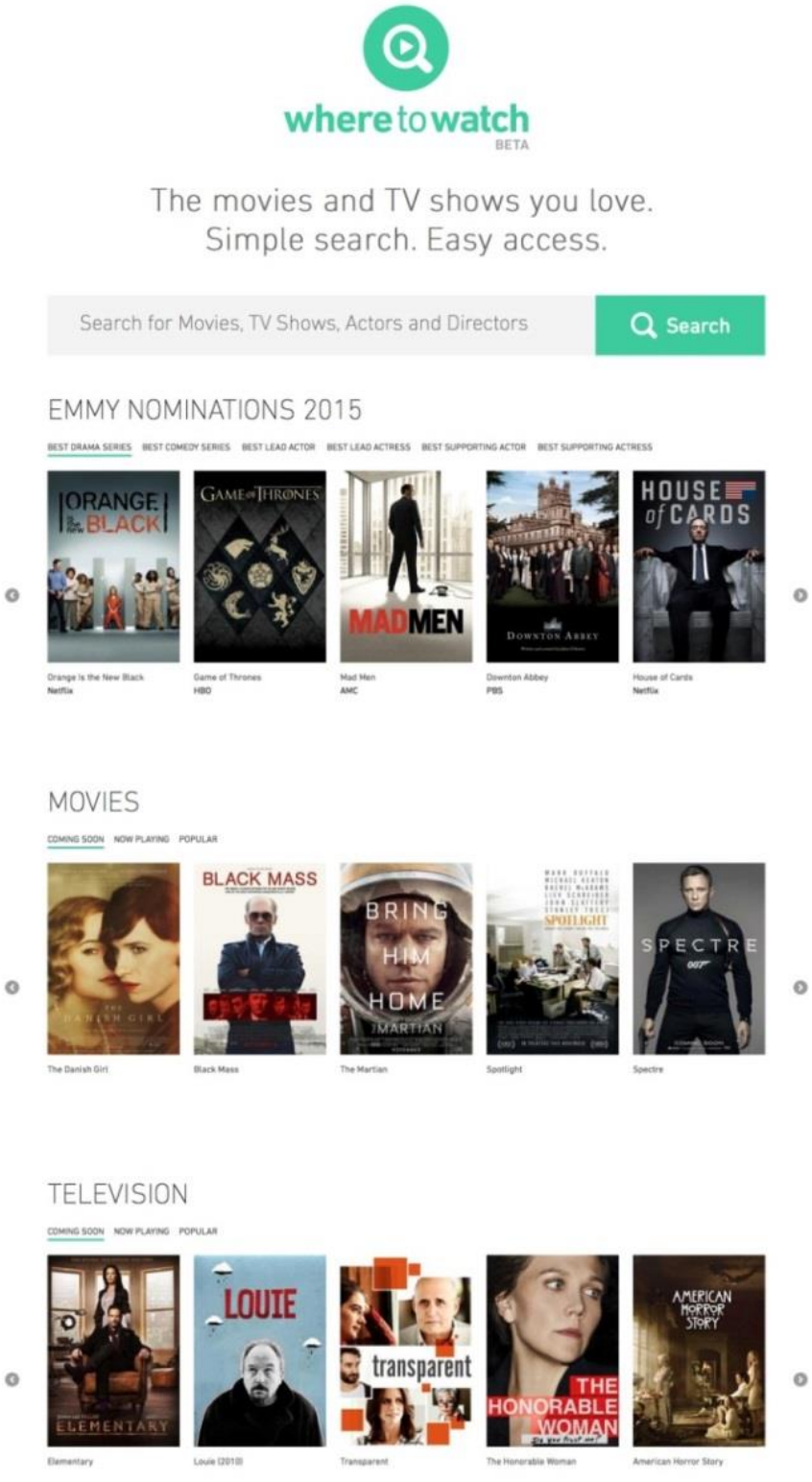
The authorized services that deliver this content to American audiences cater to every manner of consumer viewing model, including rental viewing, licensed-download, subscription viewing, and ad-supported viewing. In fact, the streaming video marketplace alone has become so robust that the FCC has already been able to subdivide it into five sub-categories: 1) subscription linear, which includes Sling TV, Sony Vue, and Verizon; 2) subscription on-demand, which includes Amazon Prime, Hulu Plus, MUBI, and Netflix; 3) transactional on-demand, which includes Amazon Instant, iTunes, VUDU, and Xbox Video; 4) ad-based linear and on-demand, which includes Crackle, Hulu, Yahoo! Screen, and YouTube Movies and YouTube TV Shows; and 5) transactional linear, which includes Ultimate Fighting Championship.[3]

In addition, the Digital Entertainment Content Ecosystem consortium of more than 60 studios, retail store chains and technology firms has created "UltraViolet," a digital rights locker for audiovisual content that allows consumers to choose their retailer while having confidence that the quality and experience will be seamless across a wide range of devices. When a consumer purchases UltraViolet media—such as a Blu-ray, DVD or Internet download—she also can access the content on any UltraViolet device registered to her household and stream the content through devices at home or on the go. Disney Movies Anywhere similarly provides a cloud-based platform for authenticating access to Disney, Marvel, Pixar and Star Wars content across multiple digital video platforms and devices, including iOS, Android, Apple TV, Chromecast, Amazon Kindle Fire and Amazon Video Fire TV, Roku, Xbox360, and web browsers. Users simply connect their Disney Movies Anywhere account to their accounts with popular digital retail services, which currently include iTunes, Google Play, VUDU, Amazon Video, and Microsoft Movies & TV. Powered by Disney's KeyChest technology, titles purchased through these participating retailers, or redeemed using the Digital Copy redemption code included in Blu-ray disc packages, are instantly and seamlessly made available to the consumer for both streaming or download across their connected accounts via the Disney Movies Anywhere apps and website.

All of this benefits consumers, who receive a high-quality viewing experience, and creators, who are able to expand their reach and monetize their enormous investments. To help viewers navigate among all the choices, as well as avoid sites that contain pirated content and may expose users to malware, identity theft, and unseemly advertising, the MPAA created WhereToWatch (www.WhereToWatch.com). WhereToWatch is a free search site that enables fans to locate television shows and films by title, actor, or director and click through to lawful online sources, as well as see show times and buy tickets for movies still in theaters.

---

[3] *See In re Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services*, MB Docket No. 14-261, *NPRM*, FCC 14-210 at ¶¶ 13, 34. (rel. Dec. 19, 2014).


where to watch
BETA
The movies and TV shows you love.
Simple search. Easy access.
Search for Movies, TV Shows, Actors and Directors
Search
EMMY NOMINATIONS 2015
BEST DRAMA SERIES
BEST COMEDY SERIES
BEST LEAD ACTOR
BEST LEAD ACTRESS
BEST SUPPORTING ACTOR
BEST SUPPORTING ACTRESS
Orange Is the New Black
Netflix
Game of Thrones
HBO
Mad Men
AMC
Downton Abbey
PBS
House of Cards
Netflix
MOVIES
COMING SOON
NOW PLAYING
POPULAR
The Danish Girl
Black Mass
The Martian
Spotlight
Spectre
TELEVISION
COMING SOON
NOW PLAYING
POPULAR
Elementary
Louie (2010)
Transparent
The Honorable Woman
American Horror Story

III. Snapshot of Online Piracy

Some claimed that pervasive online piracy would wither away once copyright industries made a robust menu of content widely and easily available online. But legitimate alternatives are now widely available and online piracy persists. An overview of the prevailing means of online content theft will help put the problem in context.

A. Direct Download and Streaming Cyberlockers

Websites that encourage users to upload content to "cyberlockers" for access by others continue to be a business model of choice for copyright thieves. The distribution process for these sites is simple: a user uploads an infringing file and the cyberlocker operator gives that user one or more links for accessing the file. The user then disseminates the links over one or more linking sites, mobile and other web applications, social media platforms, blogs, or e-mail. When someone clicks the link it initiates a download, a stream, or both. In the case of a download, that person can re-post the file on another cyberlocker site, and the cycle begins all over again.

Cyberlocker operators offering stolen content make an estimated $100 million in annual revenue, with not a penny going to creators.[4] The revenue comes from advertisements—including for major brands—that appear in association with the download or streaming activity, or from subscriptions the operator charges for faster downloads, streaming, increased data caps, or other quality improvements. They collect the subscription fees using credit card or other payment services.

In most cases, no arcane software applications or unusual technical skills are needed to enable someone to gain ready access to stolen material. At the time of a 2014 Digital Citizens Alliance study, five direct download and six streaming cyberlockers were hosted in the United States. Hosting company Webzilla hosted seven of those cyberlockers.[5]

The notice-and-takedown process for combatting cyberlockers is extraordinarily time-consuming and often ineffective. Each infringing file is associated with one or more different links, often without any overall public-facing directory identifying such files, and a cyberlocker service may offer hundreds or thousands of different links to identical infringing content. Even if you send a takedown notice on one link, other links—and the file itself—remain online. Furthermore, the evidence suggests that most cyberlockers do not strictly enforce their repeat infringer policies. For example, court records indicate that despite receiving more than eight million notifications about infringing content on its site, cyberlocker Hotfile terminated only 43 accounts, often for reasons other than infringement, and more than 60 of its users received more than 300 infringement notices but were never blocked from the site.[6]

---

[4] NetNames Report, *Behind the Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions*, Digital Citizens Alliance, at 1 (September 2014), *available at* https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/8854660c-1bbb-4166-aa20-2dd98289e80c.pdf.

[5] *Id.* at 4.

[6] *Id.* at 5.

Cyberlockers—such as 4Shared.com, BitShare.com, Rapidgator.net, Depositfiles.com, Uptobox.com, YouWatch.org, Streamcloud.eu, and Gorillavid.in[7]—are focused not on storing of files for the user, but on disseminating movies and TV shows to the public. In fact, at least 78.6 percent of files on direct download cyberlockers and 83.7 percent of files on streaming cyberlockers infringed copyright.[8] Their practice of soliciting uploads of copyrighted content, of making incentive payments to "high-value" uploaders—such as those who provide copies of movies still in theatrical release—and other characteristics distinguish them from simple cloud storage services.

B. Linking Sites

Linking sites aggregate, organize, and index links to content stored on other sites. They often host no content themselves but disseminate multiple links to "lockers," servers, or URLs on general-purpose file storage services such as Google Drive, where movies or TV content can be illegally streamed or downloaded. These sites typically use multiple or successive domain names to evade enforcement efforts. Some of the most popular sites include putlocker.is, kinogo.co, primewire.ag, and seasonvar.ru. The operators of linking sites specializing in unauthorized access to movies and TV shows often organize links by title, genre, season, and episode, using unauthorized images of the "official" cover art or poster to attract users. Depending on the website, users are commonly presented with the options of either streaming the content in a video-on-demand format or downloading a permanent copy to their device. Many popular streaming linking sites also embed video frames or video players from third-party websites, reducing the number of clicks needed to get to content for a more seamless user experience. Illicit linking sites sometimes write the source code so that the true location of the underlying content files cannot be easily identified, and thus cannot readily be reported to the hosting site. Other sites link to content posted on hosting sites or servers that they control, and refuse to remove infringing content in response to takedown notices.

The start-up costs for these sites are minimal, and advertising on the site can generate hundreds of thousands of dollars in revenue. The aggregate annual advertising revenue for linking sites in Q3 2014 was estimated at greater than $65 million, more than 15 percent of which was from premium brands.[9] Sometimes linking sites also operate cyberlocker services, thus creating an extremely lucrative business model attracting users to both platforms, and profiting handsomely through both advertising and subscriptions.

C. P2P Networks and BitTorrent Portals

Users of peer-to-peer networks—like TorrentReactor.com, torrentino.com, torrentdownloads.me, seedpeer.me, darktorrent.pl[10]—employ software that allows them to join "swarms" of other users who are sharing a particular movie, TV show, or other content. As each

---

7 *Id.* at 7.

8 *Id.* at 1.

9 Digital Citizens Alliance, *Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business*, at 3, 5 (May 2015), *available at* https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/298a8ec6-ceb0-4543-bb0a-edc80b63f511.pdf.

10 *Id.* at 24.

user downloads pieces of the file, his or her computer shares the pieces with others in the swarm. The most popular P2P software is "BitTorrent." BitTorrent websites facilitate file distribution by organizing and indexing torrent files, and initiating and managing the download process. The BitTorrent landscape remains popular, serving millions of torrents to tens of millions of users at any given time. The service is typically free to users, but the service is monetized through advertising, donations, and subscriptions.

One particularly troubling piece of P2P software is known as "Popcorn Time." Popcorn Time offers users a slick, easy-to-use interface that provides streaming of infringing, full-length copies of popular films and TV shows. Popcorn Time has become known as the "Netflix" of piracy because of its slick interface and streaming capability. In the U.K., rights holders have obtained a court order enjoining ISPs from providing users access to Popcorn Time websites. In that order, the judge noted that "[t]he point of Popcorn Time is to infringe copyright. The Popcorn Time application has no legitimate purpose."[11] Popcorn Time is open source software, and there have been multiple versions of Popcorn Time operating at any given time. Rights holders are investigating and pursuing legal remedies relating to Popcorn Time, but may need government assistance to be effective.

P2P networks remain among the top sources worldwide for unauthorized dissemination of movie content and TV programming. With the dramatic growth in bandwidth demand generated by legitimate video streaming services, the proportion of global consumer Internet traffic devoted to P2P has declined slightly, but still amounts to more than 6000 petabytes per month, representing 22 percent of all consumer video traffic on the Internet, and 18 percent of all consumer Internet traffic overall.[12] These numbers are alarming because a huge percentage of this traffic involves copyrighted content downloaded from and distributed via these networks without authorization. A 2011 technical study found that 86.4 percent of P2P traffic is infringing and non-pornographic, with infringing pornographic traffic making up a significant percentage of the remaining 13.6 percent.[13] Among the most downloaded works are illegally recorded copies of films that are still in theatrical release and television shows before they are legitimately available online or when they are made available legitimately only to subscribers of premium channels. Unauthorized downloading during these periods causes the most economic damage to content creators, which in turn discourages future investments in content creation.

D. Applications: Mobile and Connected Devices

1. Mobile Applications

Myriad mobile applications make unauthorized copies and streams of movies and television shows easily available to viewers. While the app stores operated by Google and Apple have been responsive to takedown requests regarding such apps, they remain readily available

---

[11] *Twentieth Century Fox Film Corp. v. Sky UK Limited* (2015) EWHC 1082, ¶66 (Ch).

[12] Cisco, *Visual Networking Index: Forecast and Methodology, 2014-2019*, Tables 10, 12 and 13 (May 27, 2015)(reporting 2014 figures of 21,264 PB/month for non-P2P consumer Internet video traffic and 33,595 PB/month for overall consumer Internet traffic), *available at*, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.

[13] Envisional, *Technical Report: An Estimate of Infringing use of the Internet*, at 3 (Jan. 2011), *available at* http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.

through third-party stores, for use on "jailbroken" devices, or through the use of an installer application such as "Popcorn Time." The explosive growth of the apps marketplace has spawned a new generation of more specialized search engines solely dedicated to leading consumers to stolen works. These include websites or applications that permit a user to search for a specific show or movie, and then link the user to a site where such content can be illegally obtained. Often these applications are marketed and optimized to search either for a specific type of file, such as television and movie content, or files from a particular artist. In the mobile context, these applications may include a sharing feature to promote further illegal distribution of the file.

2. Applications for Connected Devices

A host of applications for Internet connected devices such as Roku, Apple TV, Google TV, and Samsung Smart TVs facilitate on-demand streaming of pirated movies and television shows with a few clicks of a remote control. Such applications also facilitate the unauthorized live streaming of premium U.S. and international cable channels, free-to-air channels, and pay-per-view events. Some of these applications include "Plex" (plexapp.com), "Playon" (Playon.tv), and "Kodi" (Kodi.tv), which are available on the Roku Channel Store and Google Play Store/Android Marketplace. They allow installation of sub-applications—such as LetMeWatchThis, Icefilms, and Navi-x—that offer actual unauthorized streams of movies and television shows and TV channels. Multiple instructional videos available through YouTube demonstrate how to use the applications to stream for free U.S. and international cable TV channels, free-to-air channels, and PPV events.[14] Another video demonstrates how the application can be used to obtain unauthorized copies of movies and TV series.[15] Applications that enable unauthorized access are sometimes loaded into shipped "media boxes" manufactured abroad, or installed at the time of sale of the box or as an after-sale service.

E. Selling Physical Counterfeit Products Through Legitimate Online Marketplaces

Legitimate online marketplaces like Amazon and eBay are used to sell physical counterfeit copies of television shows and movies, either alone or mixed in with lawful copies. A significant volume of counterfeit physical product ends up sold on auction sites, such as eBay, and via third-party seller areas on mainstream websites, whether U.S.-based such as Amazon, Barnes and Noble, and Sears, or based overseas, such as DHGate in China. Purchases from these sites are often fulfilled through small package shipments from U.S-based sellers obtaining their inventory from overseas suppliers, which obfuscates their true origin and presents significant challenges for customs authorities to detect and interdict the illicit shipments. Individual infringing sellers also hide behind anonymous and false registrations on sites that have weak or non-existent seller-vetting procedures. Although digital dissemination presents the most pressing threat to the creative industries, hard-copy piracy and counterfeiting remains a significant problem because of the counterfeit product's high quality, including the packaging, which often makes it indistinguishable from legitimate product. Hacked set-top boxes and media boxes, as well as other devices aimed at circumventing mechanisms that control access to copyrighted works, are also found in these marketplaces.

---

[14] *See, e.g.*, Hildebrandtreview, *Free Cable on AppleTV!*, YOUTUBE, http://www.youtube.com/watch?v=77CKVV_ha14&feature=related.

[15] Polorascon, *Peliculas y series gratis con Apple TV*, YOUTUBE, http://www.youtube.com/watch?v=UrOaltyTXC8&feature=related.

IV. Solutions

Some of Congress's goals in enacting the Digital Millennium Copyright Act in 1998 have advanced more fully than others. One motivation was to provide a more certain and predictable legal environment to encourage rights holders and providers of enabling technologies and services to invest in new channels and media for disseminating creative works to a wider public. The developments summarized in Section I of this submission strongly indicate that goal has advanced. More Americans have more access to more works in more ways and with greater convenience and ubiquity than ever before.

The record is more mixed with respect to another goal of the DMCA. With the added measure of security from liability that came with qualified immunity, Congress expected digital intermediaries to work cooperatively with content creators and owners to combat IP theft occurring over those intermediaries' services and facilities. Indeed, in enacting Title II, now codified in section 512 of the Copyright Act, Congress explicitly wished 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."[16] The experiences of the 17 years since enactment have repeatedly driven home the fundamental importance of inter-industry cooperation in promoting the healthy growth of e-commerce in general, and the development of a robust online marketplace in creative works in particular.

The decentralized character of the Internet enables people all over the world to contribute to its architecture, to its functionality, and to the content that traverses its networks. By the same token, this decentralization means that, just as no one party can control the Internet, no one party can solve problems as they arise. The widespread content theft on the Internet thus demands cooperation across industries to achieve workable and effective solutions. Every responsible player in the Internet space—whether content creator, distributor, network operator, technology source, platform provider, or any of the wide range of intermediaries necessary for a successful online experience—has an obligation to contribute to these solutions. A number of promising co-operative initiatives have started to take shape. Many gaps remain, however, where key players simply have not fully stepped up to what they might reasonably be expected to do in this area.

Section 512's statutory framework embodies this emphasis on cooperation. The new structures that the statute created—notably the range of safe harbors for service providers from infringement remedies, including the notice and takedown system—all provide incentives for cross-industry cooperation "to detect and deal with" online infringement. The huge and seemingly ever-increasing volume of cases in which these structures are invoked testifies to the scope of the problem. In just the six-month period from March through August 2013, the MPAA's six member companies sent 25.2 million takedown requests to non-user generated content websites and search engines to remove infringing content located at specific URLs. Of those requests, 13.2 million were to a site to remove an infringing file and 12 million were to a search engine to remove a link from search results. These takedown notices resulted in only eight

---

[16] House of Representatives Committee on Commerce, *Report on the Digital Millennium Copyright Act of 1998*, H. Rept. 105-551, at 49, 105th Cong. 2 (July 22, 1998), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-105hrpt551/html/CRPT-105hrpt551-pt2.htm; Senate Committee on the Judiciary, *Report on the Digital Millennium Copyright Act of 1998*, S. Rept. 105-190, at 20, 105th Cong. 2 (May 11, 1998), *available at* http://thomas.loc.gov/cgi-bin/cpquery/T?&report=sr190&dbname=105&.

counter-notices, suggesting that these takedown requests were based on credible information.[17] Unfortunately, these voluminous takedown requests probably represented only a small fraction of the number of infringing files online. And even when notices result in takedowns, copies of or links to the same works often reappear on the same web site or through the same search engine within minutes because of the ease of uploading infringing content.

The MPAA believes that these statutory structures can work if parties collaborate and courts apply the framework as Congress intended, especially regarding the preconditions and criteria for claiming the safe harbors and for effectively invoking processes like notice and takedown. The MPAA and its member companies are fully engaged in these processes on a daily basis, and there may be instances in which the involvement of U.S. government agencies can help achieve greater clarity in litigation, or smoother operation of these structures in the marketplace. For now, we prefer to address issues through proper enforcement of current law, as well as in the marketplace and with voluntary initiatives. We do not rule out seeking legislative adjustments in the future, however, when circumstances demand it and if enforcement and collaborative efforts appear of no further avail.

Of greater centrality and immediacy to the next IPEC strategic plan, however, is what the IPEC and other U.S. government officials can do to promote the cooperative engagement that is essential to crafting flexible, nimble, efficient, and scalable solutions. The Office of the IPEC has made voluntary initiatives a central feature of its strategic planning. The MPAA believes it should continue to do so.

A. Voluntary Initiatives: Intermediaries Should Not Be Facilitating Piracy

Encouraging industry players to work together has been one of the IPEC's most valuable contributions to combating online copyright theft. The goal has been to craft voluntary arrangements that pool the knowledge and expertise of rights holders and other market participants, and that guide their respective actions toward the common goal of a safer, more transparent, and more trusted e-commerce marketplace. This is a goal that should be central to the long-term interests of all players. Below we discuss three voluntary initiatives that are showing particular promise, and three areas where fostering similar inter-industry initiatives should be a high priority going forward.

1. Areas of Progress

a) Internet Service Providers: the Center for Copyright Information and the Copyright Alert System

The Center for Copyright Information, a partnership between the movie and music industries and the five largest Internet service providers, represents one of the most comprehensive collaborations by the content and technology communities to combat piracy through a voluntary initiative to date. And while there is no single solution to piracy, the program is an important step in building collaborative programs through which the content and

---

[17] Boyden, Bruce, "The Failure of the DMCA Notice and Takedown System" (December 2013), *available at.* http://cpip.gmu.edu/wp-content/uploads/2013/08/Bruce-Boyden-The-Failure-of-the-DMCA-Notice-and-Takedown-System1.pdf.

technology communities can work together to protect the rights of creators and innovators. This will be an iterative process, as no program is likely to be perfect out of the box, but the Copyright Alert System shows that collaboration is possible in our efforts against piracy, and that substantial progress can be made. We continue to work with the ISPs and the music industry in this important effort.

CCI launched the Copyright Alert System in February 2013 in accord with an MOU signed by the ISPs, the MPAA, the RIAA and associations representing independent filmmakers and distributors and recording artists. The system is designed to employ a progressive series of alerts to those engaged in illegal file-sharing over P2P networks, to point them toward the growing number of ways to access digital content legally, and to educate them about the importance of protecting copyright and innovation and the problems caused by illegal downloading and file-sharing.

Under this system, content providers use publicly available IP data to notify ISPs when someone on their network, whose identity is unknown to the content provider, is engaged in unauthorized peer-to-peer downloading and distribution of copyrighted material. The ISP then sends a notice to the subscriber, without revealing his or her identity to the content provider. The initial alert simply informs the user that the infringing activity has been identified as having occurred on the subscriber's account. In the event of additionally identified infringing activity on that account, the ISP sends additional alerts requiring acknowledgement by the account holder. By the fifth and sixth instances of alleged infringement on an account, the subscriber is subject to mitigation steps at the election of the ISP, such as a reduction in service speed or the requirement to read through educational materials or to call customer service before service resumes. No account is terminated under this program. A consumer may challenge an alert if he or she believes it was sent in error, which is mentioned as part of every alert received.

The CCI released a report, "Phase One and Beyond," on May 28, 2014, that showed that 1.3 million alerts were sent out in the initial 10 months of the program.[18] More than 70 percent of these alerts were at the initial educational stages, with less than three percent of the alerts occurring at the final mitigation phase.[19] Only 265 challenges were filed under the independent review process that is managed by the American Arbitration Association and there was not one case in which an invalid notice—or false positive—was identified. Indeed, there were only 47 successful challenges in 2013, and the vast majority of those were based on an "unauthorized use of account" defense, indicating that the account holder had made a satisfactory case that someone other than the account holder or a known (authorized) person was using the account to engage in impermissible P2P downloading and distribution of copyrighted content.

During the second year of the program, the CCI has doubled the size of the program and conducted an online awareness campaign to increase public awareness of the system and its messages. The MPAA plans to work with the CCI to build on the programs' efficacy.

---

[18] Copyright Information Center, *The Copyright Alert System: Phase I and Beyond*, at 1, 4, 8 (May 28, 2014), *available at* http://www.copyrightinformation.org/wp-content/uploads/2014/05/Phase-One-And_Beyond.pdf.

[19] *Id.* at 2.

b) Payment Processors

Despite the romanticized notion of piracy as nothing more than a recreational hobby pursued mostly by teenagers, content theft is, at bottom, a lucrative criminal enterprise. Highly organized entities are engaging in it not for fun, but for profit. Significantly, only one of the thirty cyberlockers studied by Digital Citizens Alliance did not display advertising.[20] Because these "businesses" have little if any input costs, having stolen the product they sell, they generate high margins from the advertising and subscription revenue they generate on their sites. That's not to mention money they may make from any identity theft they perpetrate on visitors to their sites who provide credit card information or other data. Cutting off the money flow is thus, potentially, one of the most effective measures in combatting online piracy.

One way to restrict the money flow is for payment processors—companies such as PayPal, MasterCard, and Visa—to deny known pirate sites access to their payment networks.[21] Encouraged by the IPEC office, leading credit card companies and payment processors have agreed to work with rights holders on just such a process. While the overall impact is relatively uncertain at this point, the MPAA is encouraged by some of the steps taken thus far. PayPal, MasterCard, and Visa are working with the MPAA, with a particular focus on cyberlockers that rely on subscription services to finance their illicit operations. One challenge is "resellers"—middlemen that facilitate payments on behalf of pirate sites which have themselves been terminated from the major payment networks. As these initiatives progress, we would welcome the IPEC's continued involvement to ensure the successful application of these programs to cyberlockers and other forms of piracy that are dependent on payment processing, and to encourage other payment processors to participate, including providers of digital wallets and evolving forms of cryptocurrency that are being used increasingly as alternatives to traditional payment processing systems.

c) Ad Networks

A Digital Citizens Alliance study showed that a sample of pirate sites in 2014 derived an estimated $209 million in annual ad revenue, marking the second straight year revenues topped $200 million. The study observed ads for 132 premium brands on such sites, up from 89 in 2013. Ad revenue for illicit streaming sites is on the rise, growing 68 percent to $46.2 million, or 22 percent of total ad revenue. Profit margins range between 87 and 93 percent, even for small sites.

---

[20] NetNames Report, *Behind the Cyberlocker Door: A report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions*, Digital Citizens Alliance, at 17 (September 2014), *available at* https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/8854660c-1bbb-4166-aa20-2dd98289e80c.pdf.

[21] According to the Digital Citizens Alliance September 2014 report, Visa and MasterCard were both available payment options on 29 of the thirty sites studied. Notably, PayPal was offered as a payment option on only one cyberlocker site. NetNames Report, *Behind the Cyberlocker Door: A report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions*, Digital Citizens Alliance, at 34 (September 2014), *available at* https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/8854660c-1bbb-4166-aa20-2dd98289e80c.pdf.

MediaLink also found that infringing sites have sustained this growth, despite massive turnover and the shuttering or degrading of some of the largest sites.[22]

In 2012, independent of the IPEC, the leading associations of advertisers and advertising agencies pledged to exclude operators of online copyright theft sites from partaking in the revenue streams provided by advertising for legitimate products and services.[23] Further progress toward voluntary arrangements in the extremely complex online advertising ecosystem has continued since the last iteration of the IPEC strategic plan. A number of major players in that ecosystem—notably the Association of National Advertisers, the American Association of Advertising Agencies, and the Internet Advertising Bureau—have joined together with MPAA members, other rights holders, and technology platforms to launch the Trustworthy Accountability Group.[24] TAG's Brand Integrity Program Against Piracy aims to help advertisers and their technology partners screen out websites that present unacceptably high risks of engaging in copyright or trademark infringement, thus helping to implement a "follow the money" strategy for depriving pirates of advertising revenue.

The speed with which the TAG program is developing has been encouraging. Most recently, GroupM, the parent company of the family of WPP global media agencies, endorsed TAG and announced it would require all its media partners to become or use TAG-certified providers of anti-piracy services.[25] TAG has great potential to provide a voluntary, industry-led solution to help choke off the huge advertising revenue that makes online copyright theft financially viable today. Engagement by the IPEC could contribute to increased awareness of the TAG certification process, and its use by more advertisers and ad industry participants.

Even with TAG and other voluntary efforts underway in the online advertising space, however, key offshore ad networks continue to thrive. A relatively small number of these overseas-based networks serve advertising to most of the prominent pirate sites. These networks place display advertisements—usually the type that clutters a user's screen or tricks them into clicking a potentially harmful ad—despite having been put on notice that the sites they are doing business with are engaged in massive online theft. Because there appears to be a strong concentration of these ad networks coming out of Israel, bilateral discussions with that country could be an important aspect of an expanded effort to internationalize the voluntary arrangements that have started to make progress in this space. The well-documented links between content theft sites and cybersecurity vulnerabilities that victimize consumers provide

---

[22] Digital Citizens Alliance, *Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business*, at 2 (May 2015), *available at* https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/298a8ec6-ceb0-4543-bb0a-edc80b63f511.pdf.

[23] *See* "Statement of Best Practices Addressing Online Piracy and Counterfeiting," *available at* https://www.ana.net/content/show/id/23408.

[24] *See generally* "Fight Internet Piracy," Trustworthy Accountability Group (TAG), *available at* https://www.tagtoday.net/piracy/.

[25] *See* Tim Peterson, "GroupM Wages War on Piracy Sites with Anti-Fraud Group TAG, Demands Publishers Join," Advertising Age (Sept. 23, 2015), *available at* http://adage.com/article/digital/groupm-wages-war-piracy-sites-anti-fraud-group-tag/300510/?utm_source=mediaworks&utm_medium=newsletter&utm_campaign=adage&ttl=1443642418; https://www.tagtoday.net/groupm-requires-partners-to-use-tag-certified-anti-piracy-services/.

another compelling reason to expand ongoing efforts to deprive such sites of the financial lifeblood that comes from advertising.[26]

2. Areas in Need of Particular Attention

In the 2013 Joint Strategic Plan, the IPEC identified three additional industry sectors with particularly high potential for the development of voluntary initiatives to reduce intellectual property infringement: "data storage services, domain name registrars, and search engines."[27] For a variety of reasons, this potential has generally gone unrealized in the ensuing two years. The MPAA strongly encourages the IPEC to devote significant time, energy, and bandwidth to the development of voluntary initiatives in all three areas.

a) Domain Name Registrars and Registries

A domain name is a key resource that enables sites dedicated to digital theft to reach their customer base. Even though the terms of service for domain name registrars and registries almost uniformly prohibit the use of domain name registrations for such activities, these provisions are rarely enforced. Newly adopted provisions in their contracts with the Internet Corporation for Assigned Names and Numbers require registrars and most registries to respond to reports of illegal activities, including pervasive infringement, carried out through use of these domain names.[28] To date, however, registrars have failed to respect these provisions and ICANN has not enforced them, summarily rejecting nearly all complaints from rights holders.

The time is ripe for registrars and registries to join their industry colleagues from other sectors in embracing voluntary initiatives with rights holders to deny online copyright thieves the critical Internet resources they abuse to steal U.S. intellectual property. This is not a substitute for ICANN enforcement of the contracts it has entered into with registrars and registries. Such enforcement is sorely needed, especially as ICANN seeks to eliminate U.S. government oversight of the remaining Internet name and number management functions not already fully entrusted to it. But voluntary initiatives can provide a flexible and expeditious complement to the meaningful contract compliance efforts that ICANN needs to undertake. The ongoing launch of hundreds of new gTLDs provides additional Internet real estate for professional copyright thieves to occupy, but also the opportunity for legitimate registries to work cooperatively to combat abusive behaviors.

The multistakeholder model of Internet governance relies on two elements: 1) a transparent and credible mechanism by which the public, private sector, governments, and civil society can adopt policies, contractual agreements, and best practices to govern conduct online; and 2) respect for those policies, agreements, and practices, and a way of holding accountable

---

[26] Digital Citizens Alliance, *Selling "Slaving": Outing the Principal Enablers that Profit from Pushing Malware and Put Your Privacy at Risk*, at 2 (July 2015), *available at* https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/07027202-8151-4903-9c40-b6a8503743aa.pdf.

[27] U.S. Intellectual Property Enforcement Coordinator, *2013 Joint Strategic Plan on Intellectual Property Enforcement*, at 7-8 (June 2013), *available at* https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

[28] *See* Section 3.18.1 of the 2013 Registrar Accreditation Agreement (RAA), *available at* https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

parties who consistently breach them. Before the Internet Assigned Numbers Authority transition takes place, we must be assured of that transparency, credibility, and accountability.

Yet ICANN, registries, and registrars are not enforcing obligations created through the multistakeholder process, some dating as far back as at least 2001, that prohibit domain holders from directly or indirectly infringing the rights of others or from using domain names for illicit conduct, such as selling drugs illegally, stealing intellectual property, exploiting children, or engaging in fraudulent and deceptive practices.[29] These obligations were intensively negotiated for years, opened to the multistakeholder community for public comment, and approved by the ICANN board. The Registrar Accreditation Agreement, and the Public Interest Commitments taken on by most gTLD domain name registries, for example, require registrars and registries to prohibit domain name holders from using domain names for unlawful activity; to investigate claims of abuse; and to provide consequences for violations. Failing to enforce these provisions would jeopardize the credibility and accountability of ICANN and the multistakeholder governance model.

Despite concerns that some have voiced, enforcing these provisions would not turn ICANN into "the content police." There is an immense difference between interfering with content, speech, or political freedom on the one hand, and enforcing contract provisions prohibiting unlawful conduct on the other. Preventing the illegal sale of drugs, intellectual property theft, child exploitation, and fraud is no more a violation of free expression on the Internet than it is in the physical world. Nor would enforcing the policies raise insurmountable conflicts-of-law questions. The illegality of certain conduct, especially IP theft, is universally recognized, including in treaties. Moreover, the multistakeholder process can address any issues that do arise. The whole point of the multistakeholder model is that it creates a process for the Internet community to play a role in setting and enforcing norms and policies, including against conduct that the vast majority of nations and the global community recognize as illegal.

In recent weeks, ICANN's chief compliance officer spelled out in a blog ICANN's view of what responses would be "reasonable" for copyright owners "to expect" when they submit well-documented complaints to ICANN accredited registrars.[30] While these steps—such as notifying the domain name registrant of the complaint and seeking a response to it, which would then be passed back to the complainant—fall short of a fully "appropriate" response in many cases, they are an improvement over what registrars have been doing to date.

b) Search Engines

Search plays a unique role in the Internet ecosystem as the gateway by which most users discover and access content. Unfortunately, some search engines continue—through their search results, through suggested searches, and through sponsored advertising—to provide the pathway through which many users learn about and reach sites that engage in or facilitate online theft. Nearly three-quarters of consumers said they used a search engine for navigation or discovery in their initial viewing sessions on domains with infringing content, according to a 2013 Millward

---

[29] *See also* Sections 3.7.7 and 3.7.7.9 of the 2013 RAA, *supra* note 28.

[30] Allen R. Grogan, "Update On Steps To Combat Abuse And Illegal Activity," ICANN (Oct. 1, 2015), *available at* https://www.icann.org/news/blog/update-on-steps-to-combat-abuse-and-illegal-activity.

Brown study commissioned by the MPAA.[31] Almost 60 percent of the queries that led to infringing content contained generic or title-specific keywords only, indicating consumers were not specifically seeking infringing content. All told, search engines had a role in 20 percent of all the sessions resulting in unlawful access, equivalent to more than 300 million visits per month to a sample set of known infringing sites.

While we appreciate the effort search engines have made since the issuance of the current Joint Strategic Plan to demote in search results those sites that are clearly dedicated to, and predominantly used for, infringement, much more cooperation is needed. We continue to see illegal sites appearing all too frequently on the first page of search results, even in response to search queries that do not indicate any intent by the user to seek infringing content. And even when individual illegal sites are displaced from their peak positions in native search results, their top spots are too often assumed by similar sources of unlicensed content, resulting in no net improvement in the appearance of legitimate sites in search results.

Ideally, search engines would participate in a truly collaborative voluntary initiative, working with the content community and others to further alter the algorithms in ways that more effectively impact the results and drive consumers to legitimate sites for content. We recognize the proprietary nature of the algorithms, but there are ways to collaborate on ideas, allow search engines to experiment with them, preserve the confidentiality of specific implementation, and report out results to allow for iterative refinement before going "live." We understand that search engines have engaged in similar cooperative efforts addressing issues other than copyright infringement.

A strong and comprehensive set of best practices in the search engine area would address both the *promotion* of legitimate services, as well as the *exclusion* of confirmed bad actors from search results. Such best practices could deliver enormous benefits to all Internet players, whose interests are undermined by the prevalence of online illegal activity, and could reduce pressure for legislative or regulatory initiatives that seek the same goal. At a minimum, such practices should include:

- Demotion/Promotion. Search engines should implement effective demotion of search results pointing to copyright infringing sites, with corresponding promotion of legitimate sites to ensure that other piracy sites do not take the place of demoted sites.

- Delisting. Search engines should delist sites based on court orders or other comparable judicial determinations of infringement. Delisting in this context means that no results from a particular site would appear in any search results.

- Auto-Complete. Auto-complete functions should not guide users to search queries for infringing content or sites.

What is important to recognize is that no company is above the law and no company should facilitate illegal behavior. Search engines frequently block and prioritize results when they decide it is in their interest—or in the public good—to do so. As they do with child porn,

---

[31] Millward Brown Digital, "Understanding the Role of Search in Online Piracy" (2013), a*vailable at* http://www.mpaa.org/wp-content/uploads/2014/03/Understanding-the-role-of-search-in-online-piracy.pdf

malware, revenge porn, or merely to combat search engine optimization that they feel is against their own economic interest, search engines have the ability to configure their algorithms to prevent or mitigate certain search results. They can do this in a number of ways, such as by delinking sites, demoting sites, and adjusting how autocomplete works. The needed best practices should take these proven capabilities into account.

c) Data Storage Services

A small core of server space providers host content on behalf of websites dedicated to infringement. Often these hosting providers erect obstacles to copyright enforcement despite their obligations, under the DMCA, to respond to complaints from copyright owners. The lack of cooperation from these technology companies makes the job of enforcing rights far more difficult than it needs to be.

Closely related to hosting services are companies that provide content delivery networks, distributed DNS service, and associated security and optimization services to websites. The most prominent example is the U.S. company Cloudflare. While these companies provide many valuable services to legitimate websites, they also provide them to sites dedicated to copyright theft. The services they provide obfuscate the Internet Protocol addresses of the hosts of sites, thus impeding enforcement efforts against those sites that exist solely to infringe. These companies also too often refuse to enforce their own terms of service to cut off support for clearly illegal sites. By bringing companies in this sector to work out voluntary arrangements with rights holders for quickly revealing the actual hosting service and denying further services to the worst offenders, the IPEC could make a material contribution to a safer e-commerce marketplace and to the healthy growth of trade in copyrighted creative content.

B. Law Enforcement

While voluntary initiatives provide a forum in which responsible players can come together to craft pragmatic solutions, robust law enforcement capability is still needed to deal with those for whom the online environment is simply an attractive venue for theft and abuse. One of the core goals of the IPEC strategic plan must be to ensure that the finite but highly significant resources and expertise of federal law enforcement agencies are deployed as efficiently as possible to deliver the maximum "bang for the buck" against criminal enterprises operating online to steal U.S. intellectual property. In particular, the coordination across U.S. federal agency lines, and the outreach to and collaboration with like-minded authorities in other countries, that have characterized successful law enforcement initiatives such as Operation In Our Sites and the coordinated prosecution of Kim Dotcom and his Megaupload confederates, provide an excellent model for ambitious and well-prepared enforcement actions in the future. Curtailing piracy will boost lawful commerce in creative works. For example, when the Department of Justice shut down Megaupload—then the largest piracy "cyberlocker," accounting for four percent of all Internet traffic—digital sales for three major studios in 12 countries increased between 6.5 and 8.5 percent, according to a Carnegie Mellon study.[32]

One of the challenges facing law enforcement is that most of the individuals engaged in online theft of film and TV intellectual property are located outside the United States. These

[32] Brett Danaher and Michael D. Smith, *Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales* (Sept. 14, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229349.

enterprises nonetheless steal American intellectual property, target U.S. citizens, and in some cases have financial assets within our borders. Federal law enforcement agencies and rights holders need to work together to develop a law enforcement strategy that can have a meaningful impact on these enterprises.

Finally, we note the Administration's repeated call to close the loophole that treats unauthorized Internet streaming differently than unauthorized downloading in criminal cases. As the Justice Department has noted in congressional testimony, because willful infringement of the public performance right can only be penalized as a misdemeanor, the statute yields an insufficient response in the case of sites "willfully streaming pirated content to large numbers of users, and turning huge profits through advertising revenue and subscriptions." Closing this loophole and adding a felony penalty would provide "an important tool to prosecute and deter" such conduct.[33] The MPAA agrees with the conclusion of the Register of Copyrights that such an amendment is "warranted and overdue."[34]

---

[33] *See* Statement of David Bitkower, Acting Deputy Assistant Att'y Gen., Crim. Div., U.S. Dep't of Justice, *Copyright Remedies: Hearing Before the Subcomm. on Courts, Intellectual Prop. & the Internet of the H. Comm. On the Judiciary*, 113th Cong. 2 (2014), at 7-8, *available at* http://judiciary.house.gov/_cache/files/c2cf069f-5e3d-4449-8614-c05b183fd910/bitkower-doj-remedies-testimony.pdf.

[34] *See* Statement of Maria A. Pallante, Register of Copyrights and Dir., U.S. Copyright Office, *The Register's View on Copyright Review: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 19 (2015), *available at* http://judiciary.house.gov/_cache/files/9855f607-e28b-4ff9-b2f6-7a1106d4ce48/114-22-94408.pdf.