Before the
Intellectual Property Enforcement Coordinator
Washington, D.C. 20502

In the Matter of	)
	)
Development of the Joint Strategic Plan	)
on Intellectual Property Enforcement	)
	)
Request for Written Submissions	)

Comments of the Motion Picture Association of America, Inc.

Nov. 13, 2018

Neil Fried
SVP & Senior Counsel
Motion Picture Association of America, Inc.
1301 K Street NW, Washington, D.C. 20005
(202) 378-9100

Table of Contents

Overview

American audiences have never had more choices in the movies and television shows they can enjoy—or when, where, and how to enjoy them. Much of this results from our nation's respect for copyright, which encourages the production of U.S. content and its wide dissemination at home and abroad. That benefits audiences, helps drive American innovation, produces well-paying jobs, and grows the local and national economies.

Piracy remains a problem, nonetheless, as illegal enterprises enlist online tools to facilitate unauthorized dissemination of content on a global scale. Compounding matters is the lack of accountability of some major online platforms for their failure to prevent content theft and other illicit conduct over their services. By creating a less hospitable environment for individuals and businesses to engage in commerce and creativity, and forcing legitimate firms to compete with unlawful actors, that lack of accountability harms consumers, growth, and American competitiveness.

The MPAA thus welcomes the Administration's approach of treating "America's inventive and creative capacity as something [to] protect, promote, and prioritize."[1] To that end, and consistent with the Administration's four-part approach to promoting and protecting intellectual property by: 1) engaging with America's international partners; 2) using all its legal authorities, including trade tools; 3) expanding law enforcement action and cooperation; and 4) partnering with the private sector and other stakeholders,[2] the MPAA asks the IPEC to:

- work with the National Telecommunications and Information Administration to restore and preserve access to WHOIS data, which law enforcement, the private sector, and public interest groups use to combat illicit online activity, including not only the theft of intellectual property, but also sex trafficking, unlawful sale of opioids, cyber-attacks, and identity theft;

- push for trade agreements that raise the international level of copyright protection and enforcement, that reduce market barriers to U.S. movies and television programming, and that refrain from expanding online immunities, which lessen incentives for online platforms and internet intermediaries to proactively curb online lawlessness;

- encourage additional efforts by the DOJ, Immigration and Customs Enforcement, Customs and Border Protection, the FTC, the FCC, and other relevant departments to combat piracy, which harms consumers, competition, and cybersecurity; and

- continue encouraging internet intermediaries to engage in voluntary, collaborative initiatives to more proactively curb the mass, unauthorized dissemination of copyrighted works.

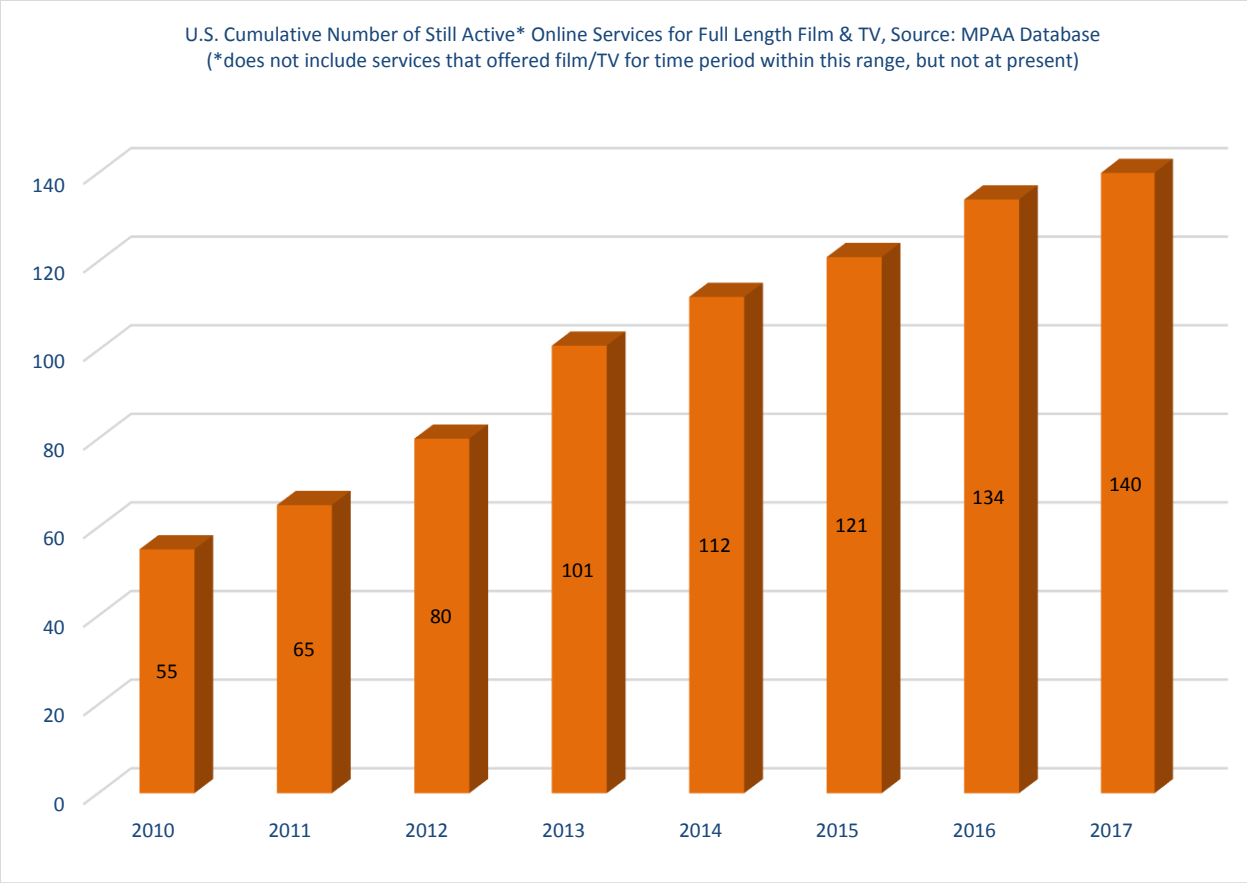
---

[1] *In re* Development of the Joint Strategic Plan on Intellectual Property Enforcement, *Request for Written Submissions*, 83 Fed. Reg. 46522, 46523 (Sept. 13, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-09-13/pdf/2018-19863.pdf.

[2] *Id.* at 46523.

I. Americans Are Continuing to Enjoy Another Golden Age of Movies and Television

American viewers are benefitting from unprecedented competition for movies and television programming—not only in theaters and over broadcast, cable, and satellite services, but also online, as the following three charts indicate. The U.S. film and TV industry releases more than 450 movies and nearly 500 scripted shows per year.[3] The industry makes that content available to American audiences through 140 lawful online film and TV services as of 2017, up from 80 in 2012.[4] U.S. viewers used those services, many of which have become global powerhouses, to access 163.1 billion movies and TV episodes in 2017, up from 51.6 billion in 2012.[5] The number of scripted shows reached 487 in 2017, up from 288 in 2012. Of those 487 shows, 117 were created for online outlets, compared to just 15 shows five years earlier.[6]

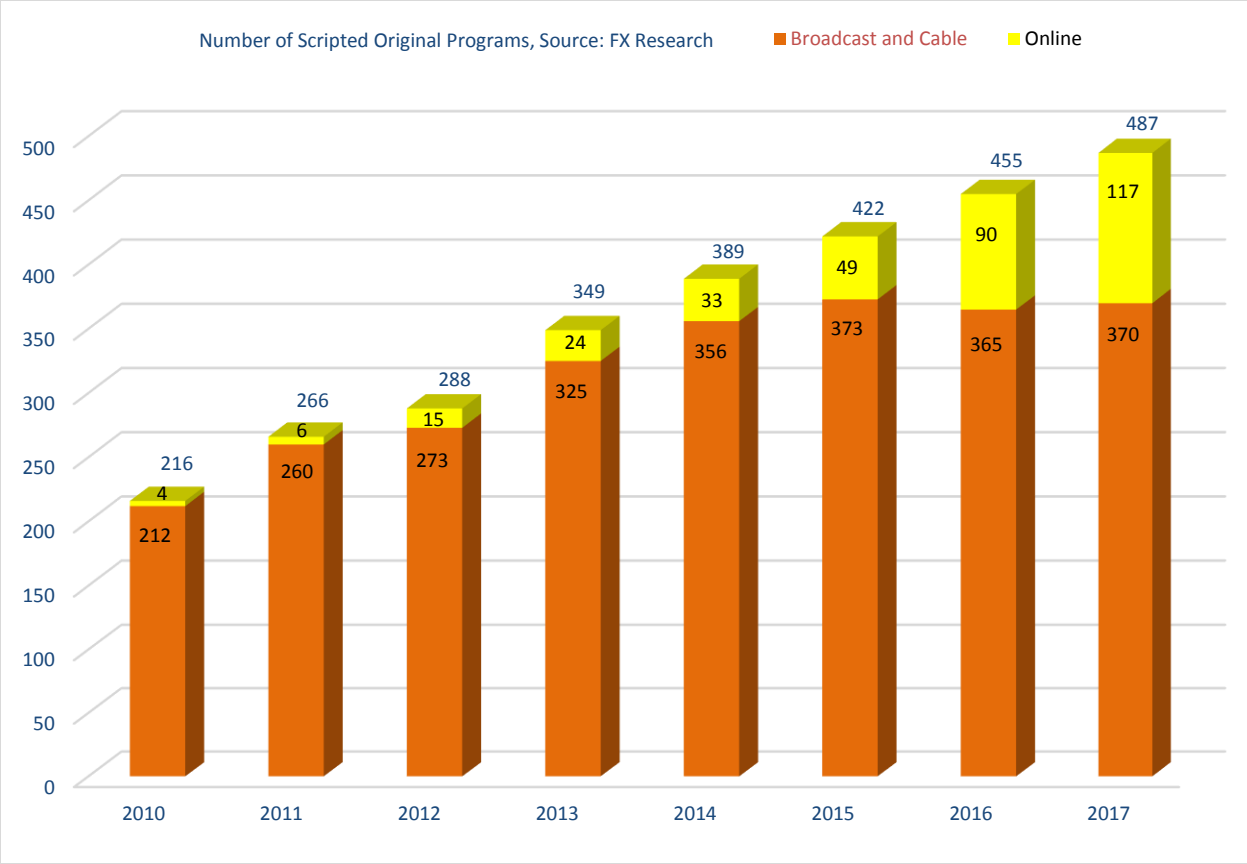


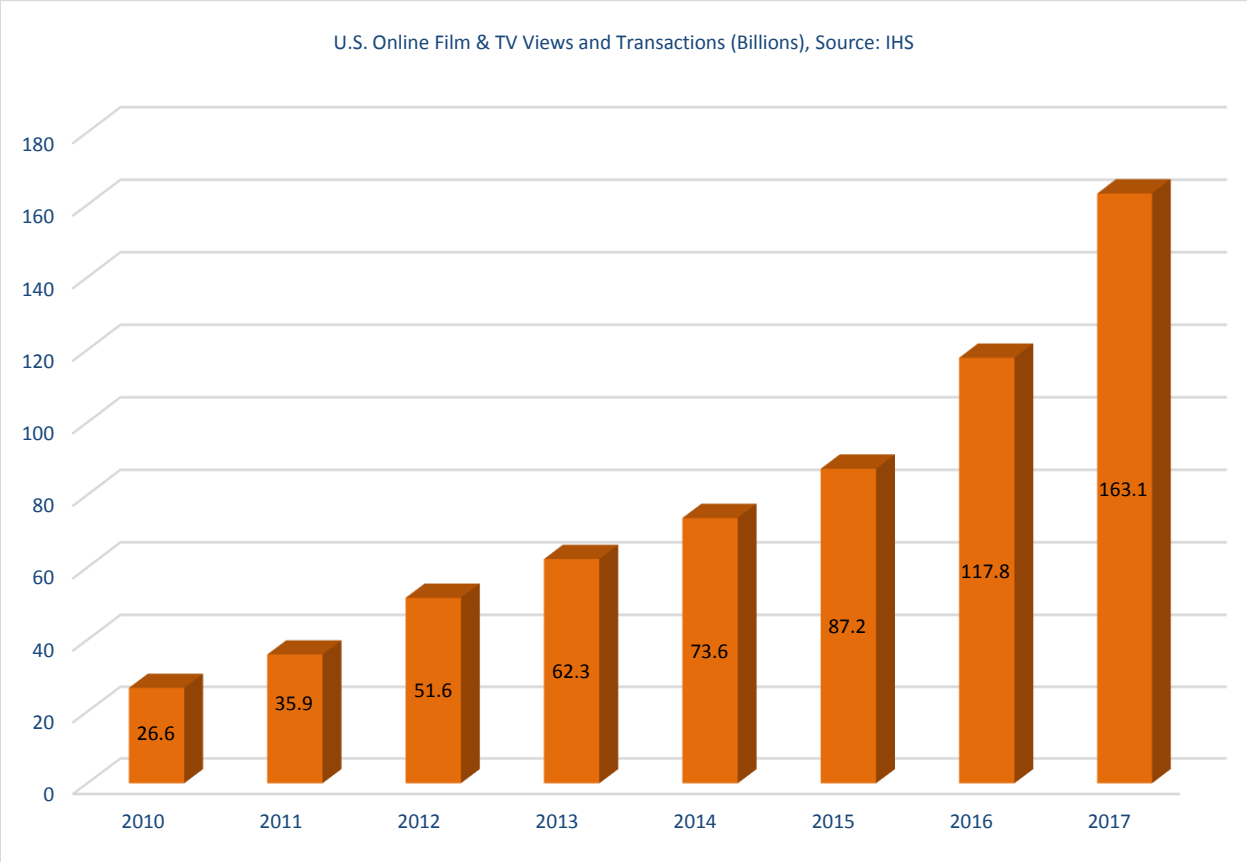
[3]MPAA, 2017 THEATRICAL HOME ENTERTAINMENT MARKET ENVIRONMENT REPORT (2018) (using data for U.S. country-of-origin movies only), https://www.mpaa.org/research-docs/2017-theatrical-home-entertainment-market-environment-theme-report/; Joe Otterson, *487 Scripted Series Aired in 2017, FX Chief John Langford Says*, VARIETY, Jan. 5, 2018, https://variety.com/2018/tv/news/2017-scripted-tv-series-fx-john-landgraf-1202653856/.

[4]MPAA database.

[5]IHS Markit. *See* www.IHS.com.

[6]FX Networks Research (2018).


Number of Scripted Original Programs, Source: FX Research
Broadcast and Cable
Online
500
450
400
350
300
250
200
150
100
50
0
216
4
212
266
6
260
288
15
273
349
24
325
389
33
356
422
49
373
455
90
365
487
117
370
2010
2011
2012
2013
2014
2015
2016
2017


U.S. Online Film & TV Views and Transactions (Billions), Source: IHS
180
160
140
120
100
80
60
40
20
0
26.6
35.9
51.6
62.3
73.6
87.2
117.8
163.1
2010
2011
2012
2013
2014
2015
2016
2017

As audiences benefit from this activity so, too, do America's national and local economies. In the process of making content available online and off, the television and film industry supports 2.1 million jobs and $139 billion in wages across all 50 states; enlists more than 93,000 businesses, 87 percent of which are small businesses employing fewer than 10 people; and contributes $134 billion in sales.[7] In addition, the industry pays $49 billion to 400,000 local businesses.[8] A major motion picture filming on location contributes on average $250,000 per day to the local community, and a one-hour television episode contributes $150,000 per day. Notably, the local community enjoys that up-front financial injection regardless of whether the film or TV show becomes a hit or a flop.

II. Respect for Copyright Drives Innovation and Competition

Respect for copyright helps drive this creative and economic activity, making the United States the global leader in the creation of content enjoyed worldwide. The Constitution's Copyright Clause recognizes that securing the rights of creators in the fruits of their creativity, including to determine how to disseminate their works, increases both the production and distribution of content, to the ultimate benefit of the public.[9]

The exclusive rights of creators to protect, disseminate and license their content helps manage the economic risks in the ultra-competitive video marketplace. Producing and distributing a major motion picture costs on average $100 million, and six out of ten *never* make back their initial investment. Major television productions now rival feature films not only in quality, but also in cost, reaching millions of dollars *per episode*. Yet, according to an industry rule of thumb, 80 percent of scripts never become a pilot, 80 percent of pilots never become a series, and 80 percent of series never see a second season, reinforcing the high risk of this creative business.

The ability of content owners and distributors to use technological protection measures—sometimes referred to as digital rights management—enables them to offer a wide variety of innovative viewing options at different price points. Because of these technological measures, audiences can choose how to access programming, including by downloading content to a hard drive, streaming content for a limited time on a pay-per-view basis, enjoying content as part of a subscription service, watching content over TV Everywhere applications in different places across different devices, and accessing full seasons of a television series, either to catch up with past episodes or to watch them all at once when a content creator makes them available *en masse* from the start. Without technological protection measures to provide effective differentiation among offerings and to ensure viewers gain access to the programming on the terms authorized, content

---

[7] MPAA, THE ECONOMIC CONTRIBUTION OF THE MOTION PICTURE & TELEVISION INDUSTRY TO THE UNITED STATES (NOV. 2017), https://www.mpaa.org/wp-content/uploads/2018/03/MPAA-Industry-Economic-ContributionFactsheet_2016-FINAL-2.pdf.

[8] *Id.*

[9] *See* U.S. CONST., art. I, § 8, cl. 8 (conferring upon the legislative branch the role "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries"); *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 558 (1985) (stating that "[b]y establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas.").

creators would not be able to offer all these choices through various outlets at various points in the distribution cycle.

III. Piracy Continues to Harm Consumers and Competition

Although physical-goods-based piracy remains a persistent threat in many parts of the globe, unauthorized distribution online is frequently extra-jurisdictional in reach and has the most significant impact on the worldwide market for U.S. movies and television programming. In the past, many copyright skeptics claimed that pervasive online piracy would wither away once copyright industries made a robust menu of content widely and easily available online. But despite the U.S. motion picture and television industry's embrace of the internet as a powerful way to reach audiences through lawful services, online piracy remains a drag on American content production and innovation.

Content thieves take advantage of a wide constellation of easy-to-use online technologies, such as direct download, streaming, and piracy applications, usually for monetary gain. These sites and services often have the look and feel of legitimate content distributors, luring unsuspecting consumers into piracy. An estimated 542 million pirated movies and TV shows were downloaded in the United States in 2017 using peer-to-peer protocols alone.[10] Streaming piracy has now surpassed illicit downloading via peer-to-peer protocols, with streaming piracy sites representing 37 percent of visits to sites with unauthorized content, compared to 36 percent for sites hosting downloadable files of infringing content and 27 percent for peer-to-peer sites.[11]

An emerging global threat is piracy from illegal internet protocol television services that provide stolen telecommunication signals or channels to a global audience via dedicated web portals, third-party applications, and piracy devices configured to access the service. The MPAA has identified more than one thousand of these illegal IPTV services operating around the world.

Piracy devices preloaded with software to illicitly stream movies and television programming and a related ecosystem of infringing add-ons continue to be problematic, although enforcement actions against key targets are having an impact. Websites enable one-click installation of modified software onto set-top boxes or other internet-connected devices. This modified software taps into an ecosystem of infringing content add-ons and portals to illicitly stream movies and television programming live or "on demand."

The following overview of the ecosystem surrounding the theft and unauthorized dissemination of copyrighted movies and television shows will help put the problem in context:[12]

---

[10]MarkMonitor. *See* www.markmonitor.com.

[11]Analysis of SimilarWeb data, based on sites with at least 10,000 copyright removal requests in 2017 according to the Google Transparency Report.

[12]For illustrative examples, *see In re* Request for Public Comment on the 2018 Special 301 Out of Cycle Review of Notorious Markets, Docket No. USTR-2018-0027, MPAA Comments (Oct. 1, 2018), *available at* https://www.mpaa.org/policy-statement/mpaa-comments-to-ustr-on-notorious-markets/.

Linking and Streaming Websites. Linking sites aggregate, organize, and index links to content stored on other sites. Linking sites that offer unauthorized access to movies and TV shows typically organize posts by title, genre, season, and episode, and often use the official, copyright-protected art to advertise the content. The sites then provide one or more active links so users can access the infringing content. 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 computers. Many streaming link sites also frame or embed video players from third-party websites, reducing the number of clicks needed to get to content while retaining the user to serve advertisements. Some also appear to be hosting the underlying content files on servers they control to maintain continuity of infringing offerings and to avoid takedowns on third-party file-hosting sites. They largely derive their revenue from advertising and referrals.

Direct Download Cyberlockers and Streaming Video Hosting Services. Direct download cyberlockers and streaming video hosting services are websites that provide centralized hosting for infringing content that the public can downloaded or stream. The distribution process is simple. A user uploads an infringing file and the cyberlocker or video hosting service gives the user a link for accessing the file. The user posts the link on one or several linking sites. Clicking the link will initiate a download or stream of the uploaded file. Links for unauthorized copies of movies and television programs are widely disseminated across the internet, not just via linking sites, but also via mobile and other web applications, social media platforms, forums, blogs, and email. Complicating enforcement, cyberlockers and video hosting services frequently provide several unique links to the same file and use proxy services to mask where the site and content are hosted. If a content owner sends an infringement notice for one of the links, the others may remain active, enabling continued infringement. Additionally, many cyberlockers and video hosting services do not respond at all to takedown notices. According to a NetNames and Digital Citizens Alliance report, "[u]nlike legitimate cloud storage services … the cyberlocker business model is based on attracting customers who desire anonymously to download or stream popular, copyright infringing files that others have posted."[13] NetNames found that the 30 direct download and streaming cyberlockers it analyzed took in close to $100 million in total annual revenue and generated average profit margins of 63 to 88 percent from a mix of advertising and subscription services.[14] The principle use and purpose of these cyberlockers is to facilitate content theft. By making vast amounts of infringing premium content available to the public, these sites attract huge amounts of traffic.

Illegal Internet Protocol Television Services. Illegal internet protocol television services typically offer hundreds of channels illegally sourced from providers worldwide, alongside video-on-demand content that includes unauthorized copies of movies and television

[13]NETNAMES, BEHIND THE CYBERLOCKER DOOR: A REPORT ON HOW SHADOWY CYBERLOCKER BUSINESSES USE CREDIT CARD COMPANIES TO MAKE MILLIONS (Sept. 2014), http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=cyberlockers.

[14]*Id.*

series. Many of these illegal services are subscription based and run for profit, offering monthly or yearly packages to their user base. The technical infrastructure related to these services is often vast and complex, making the identification of content sources and service operators extremely challenging. The marketing and sale of these services is often carried out by a network of global re-sellers who purchase subscriptions at wholesale prices and re-sell them for a profit, further complicating investigations. To function, illegal internet protocol television services must rely on infrastructure and support services, such as hosting providers, media servers, and panel hosting. Some of the infrastructure and support services are unaware of the underlying illegal activity. Others, however, tailor their business strategies towards illegal sites or look the other way, even when informed, themselves becoming bad actors.

Piracy Devices and Applications. A damaging piracy ecosystem has emerged around piracy devices and applications, sometimes referred to as "illicit streaming devices." The devices, often Android-based "set-top boxes," are sometimes built around Kodi open-source media software. The applications connect users to streams of stored or "live" pirated movies and television programming, and enable "plug and play" connection to a standard television set, thus undermining the licensing fees paid by distributors on which content creators depend. Six percent of North American broadband households—some 6.5 million homes—are accessing known subscription television piracy services, according to Sandvine.[15] A rough estimate by Sandvine suggests the streaming device piracy ecosystem may be generating ill-gotten gains of $840 million per year in North America, a number that may well be understated.[16] Streaming devices preloaded with infringing applications and TV/VOD subscription services can be found online and in physical marketplaces. Additionally, illegal applications that can make legitimate streaming devices infringing can be found through a myriad of legitimate and specialty app repositories.

Peer-to-Peer Networks & BitTorrent Portals. Users of peer-to-peer or file-sharing networks use software that allows them to join "swarms" of other users who are distributing a particular title, such as a movie, TV show, or book. As each user downloads pieces of the file, his or her computer distributes the pieces to others in the swarm. The most popular peer-to-peer 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 or tens of millions of users at any given time.

Hosting Providers. Hosting providers make available the essential infrastructure required to operate a website. Websites engaged in massive copyright infringement depend on a hosting provider to make their websites easily viewable and to provide high-quality

[15] SANDVINE, SPOTLIGHT: SUBSCRIPTION TELEVISION PIRACY 2 (Nov. 2017), https://www.sandvine.com/hubfs/downloads/archive/2017-global-internet-phenomena-spotlight-subscription-television-piracy.pdf.

[16] *Id.*

streaming videos. The hosting provider has the ability to take websites engaged in massive copyright infringement offline or to disable or otherwise shut them down. Some hosting providers allow sites to hide behind a content delivery network. A content delivery network is typically used to effectively and efficiently deliver content to a global user base by placing servers all around the world that cache the pages of the website, providing a high-speed hosting infrastructure to some of the most popular web streaming services. One of the by-products of using a content delivery network is that they mask the true IP and hosting provider of a website. Given the central role of hosting providers in the online ecosystem, it is disconcerting that many refuse to take action when notified that their hosting services are being used in clear violation of their own terms of service prohibiting intellectual property infringement and in blatant violation of the law.

Ad Networks. The companies connecting advertisers to infringing websites inadvertently contribute to the prevalence and prosperity of infringing sites by providing funding to the operators of these sites through advertising revenue. Although many ad networks have established best practices and guidelines to address ads supporting or promoting piracy, detection and policing of illicit sites continues to have its challenges.

Physical Counterfeit Products. Although digital dissemination presents the most pressing threat to the creative industries, hard-copy piracy and counterfeiting remains a problem because of the counterfeit products' high quality, including the packaging, which often makes it indistinguishable from legitimate product. These products can be purchased from websites and online sales platforms, sometimes even legitimate ones, and are often fulfilled through small-package shipments from U.S.-based sellers obtaining their inventory from overseas, which obfuscates their 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.

All these forms of infringement harm a broad swath of the legitimate movie and television production and distribution sectors, including content creators, large and independent movie and television studios, production crews, small businesses that support productions, sports leagues, broadcast and pay-TV networks and distributors, and over-the-top video services. The illicit activity unlawfully competes with digital entrepreneurs and established players trying to grow lawful and innovative content and distribution businesses. The large-scale availability of pirated content makes it harder for legitimate content companies and distributors to earn a return on investment, and thus also discourages some of that investment in the first place. Moreover, by diverting subscribers from these legitimate services and siphoning financial returns that would otherwise be available to re-invest in creative content, piracy harms competition and limits the ability of content creators and distributors to offer innovative choices in movies, television programming, and other video services.

Such piracy also harms consumers, both because it interferes with the public benefits derived from copyright protection and because it directly imposes risks of other consumer harms.

For example, as companies have focused resources on ensuring their advertising does not appear on pirate sites, those sites have increasingly used the pirated content as bait for identity theft and malware distribution as an alternative source of revenue. Indeed, one-third of pirate sites expose users to malware and pirate sites are 28 times more likely to infect users with malware than mainstream websites.[17] Further, a March 2018 Carnegie Mellon University study found that doubling the amount of time spent on infringing sites causes a 20 percent increase in malware count.[18] Such risks jeopardize the general public and legitimate digital trade. The spread of piracy thus presents a growing threat not only to commerce, but also to consumers, the health of the internet, and cybersecurity.

IV. To Further Drive American Competitiveness, Combat Cyber-Threats, and Protect Consumers, the MPAA Asks the IPEC to Help Ensure Continued Access to WHOIS Data, to Push for Trade Agreements with Strong Copyright Provisions, to Advance Federal Agency Efforts to Combat Streaming Piracy, and to Encourage Internet Intermediaries to Engage in Voluntary Initiatives to Stem Content Theft

The IPEC seeks input regarding the U.S. government's intellectual property enforcement efforts, broken down by the Administration's four-part approach to promoting and protecting intellectual property: A) engagement with international partners; B) use of legal authorities, including trade tools; C) law enforcement action and cooperation; and D) engagement with the private sector and other stakeholders.[19] Along those lines, the MPAA asks the IPEC to:

- work with the NTIA to restore and preserve access to WHOIS data, which law enforcement, the private sector, and public interest groups use to combat IP theft and other forms of illicit online activity, such as sex trafficking, illegal sale of opioids, cyber-attacks, and identity theft;

- push for trade agreements that raise the international level of copyright protection and enforcement, that reduce market barriers to U.S. movies and television

---

[17] DIGITAL CITIZENS ALLIANCE, DIGITAL BAIT 2 (Dec. 2015), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf. *See also* EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE, IDENTIFICATION AND ANALYSIS OF MALWARE ON SELECTED SUSPECTED COPYRIGHT-INFRINGING WEBSITES 3 (2018) (stating that copyright infringing websites "commonly distribute various kinds of malware and potentially unwanted programs (PUPs), luring users into downloading and launching these files"), https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Malware_Study/2018_Malware_Study_en.pdf.

[18] RAHUL TELANG, DOES ONLINE PIRACY MAKE COMPUTERS INSECURE? EVIDENCE FROM PANEL DATA (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3139240.

[19] *In re* Development of the Joint Strategic Plan on Intellectual Property Enforcement, *Request for Written Submissions*, 83 Fed. Reg. 46522, 46523 (Sept. 13, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-09-13/pdf/2018-19863.pdf.

programming, and that refrain from expanding online immunities, which lessen incentives for online platforms and intermediaries to proactively curb lawlessness;

- encourage additional efforts by the DOJ, Immigration and Customs Enforcement, Customs and Border Protection, the FTC, the FCC, and other relevant departments to combat piracy, which harms consumers, competition, and cybersecurity; and

- continue encouraging internet intermediaries to engage in voluntary, collaborative initiatives to more proactively curb the mass, unauthorized dissemination of copyrighted content.

A. The IPEC Should Work with the NTIA to Preserve Access to WHOIS Data

WHOIS data—which contains contact information about domain name registrants—has been a cornerstone of online security and safety since before the dawn of the commercial internet.[20] Access to such information is critical to: 1) creating the transparency, accountability, and trust consumers need to be willing to share their data in the online environment; 2) protecting consumers from online lawlessness—including not only IP theft but also sex trafficking, unlawful sale of opioids, cyber-attacks, and identity theft; and 3) maintaining the hospitable online environment necessary to promote internet communication, commerce, and creativity.

Unfortunately, the Internet Corporation for Assigned Names and Numbers has enacted a Temporary Specification[21]—under the stated goal of complying with the European Union's General Data Protection Regulation—that is unnecessarily resulting in restricted access to important WHOIS data well beyond what the GDPR mandates, and not just in Europe, but also in the United States and elsewhere. The GDPR does not apply at all to non-personal information;[22] and even in the case of personal information, the regulation acknowledges legitimate interests can warrant collection and disclosure, such as public safety, law enforcement and investigation, enforcement of rights or a contract, fulfillment of a legal obligation, cybersecurity, and preventing fraud.[23] Moreover, the GDPR does not apply to American registrars and registries with respect to domain name registrations by U.S. registrants, or where domain name registrants and registrars are located outside the European Economic Area.[24] Furthermore, it applies only to information about "natural persons," and so imposes no obligation to obfuscate information about domain

---

[20] *See History of WHOIS*, ICANN WHOIS, https://whois.icann.org/en/history-whois (last visited Nov. 7, 2018).

[21] ICANN, TEMPORARY SPECIFICATION FOR GTLD REGISTRATION DATA (May 25, 2018), https://www.icann.org/resources/pages/gtld-registration-data-specs-en.

[22] *See* GDPR, arts. 1 (describing the subject matter and objectives of the regulation as relating to the processing and protection of personal data), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[23] *See id*., arts. 2(2)(d), 5(1)(b), 6, 23. *See also* ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—San Juan, Puerto Rico* (Mar. 15, 2018) (stating that the GDPR allows for access to data for legitimate purposes), https://gac.icann.org/advice/communiques/20180315_icann61%20gac%20communique_finall.pdf.

[24] *See* GDPR, arts. 2(2)(a), 3.

name registrants that are companies, businesses, or other legal entities, irrespective of the nationality or principal place of business of such entities.[25] Applying any GDPR-related restrictions on the WHOIS data of domain name registrants other than natural persons that are residents of the EEA or who register domains with EEA registrars thus goes beyond the regulation's scope and is already harming consumer protection, public safety, and cybersecurity, as government entities, the private sector, and public interest groups are warning.[26] For example, inconsistent implementation of ICANN's Temporary Specification and confusion among registrars and registries has impeded attempts to investigate and mitigate cyber-attacks, according to a joint analysis of more than 300 survey responses by the Anti-Phishing Working Group and the Messaging, Malware, and Mobile Anti-Abuse Working Group.[27]

Now is the time to be increasing online transparency, not diminishing it. The MPAA therefore asks the IPEC to work with the NTIA to ensure that certain basic WHOIS information remains publicly available, and that any information that the GDPR does require to be removed from public access still be available to third parties with legitimate interests through a reasonable, timely, and effective process. The IPEC and the NTIA should take an "all of the above" approach and help advance a variety of contemporaneous efforts to ensure continued WHOIS access, including through diplomatic channels, the ICANN multistakeholder process, trade agreements, and U.S. legislative action.

For example, the MPAA urges the Administration to continue reiterating the importance of access to WHOIS data and the problems associated with ICANN's overbroad application of the GDPR,[28] and to ask European policymakers and data protection authorities to clarify that the

---

[25]*See* GDPR, art. 1 (describing the subject matter and objectives of the regulation as relating to the protection of natural persons. *See also GAC Communiqué* (stating that the GDPR applies only to the privacy of natural persons, not legal entities).

[26]*See e.g., GAC Communiqué*; Letter from more than 50 national and international organizations, trade associations, companies and non-profit entities to Article 29 Working Party, European Commission (March 5, 2018), https://www.icann.org/en/system/files/files/gdpr-comments-sheckler-et-al-article-29-wp-whois-05mar18-en.pdf.

[27]ANTI-PHISHING WORKING GROUP & MESSAGING, MALWARE AND MOBILE ANTI-ABUSE WORKING GROUP, ICANN GDPR AND WHOIS USERS SURVEY 4 (Oct. 2018), *available at* https://apwg.org/apwg-news-center/icann-whois-access/temporySpecSurvey and https://www.m3aawg.org/rel-WhoisSurvey2018-10.

[28]*See, e.g.*, Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 61 (Mar. 12, 2018) (stating that "the WHOIS service is an incredibly valuable tool for governments, businesses, intellectual property rights holders, and individual Internet users around the world," supporting "a solution that maintains the WHOIS service to the greatest extent possible in the face of data protection and privacy regulations such as the European General Data Protection Regulation," expressing a need to "maintain[] a WHOIS service that is quickly accessible for legitimate purposes," encouraging "revisions to [ICANN's interim] model to permit access to the most amount of registration data as possible," voicing "concern[] with the uncertainty around how access to WHOIS information for legitimate purposes will be maintained in the period between the date of GDPR enforcement, May 25, and the time in which the community is able to develop and agree to a formal accreditation process," calling for "[p]lans … to be put in place to ensure that the users behind the already defined legitimate purposes—such as law enforcement, intellectual property enforcement, and cybersecurity—are not stymied in their efforts to serve the public interest," and saying that "[t]he United States will not accept a situation in which WHOIS information is not available or is so difficult to gain access to that it becomes useless for the

GDPR does not prevent access to WHOIS data in the European Economic Area for legitimate law enforcement, consumer protection, and enforcement of rights purposes. The MPAA also asks the IPEC to convey to registrars and registry operators that it expects them to continue making WHOIS data publicly available outside the applicable reach of the GDPR. In the category of multistakeholder efforts, the IPEC and the NTIA should urge ICANN and stakeholders to accelerate work on adopting a post-GDPR WHOIS-solution through the Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data.[29] The IPEC and the NTIA should also continue to support efforts to provide access to non-public WHOIS data through an accreditation and access model, including the proposal from ICANN for a unified access model, or through other means that ICANN has suggested exploring, such as ICANN assuming legal responsibility for providing access as a sole controller.[30] On the trade side, the Administration should seek robust WHOIS access requirements in future trade agreements, perhaps expanding on language included in the U.S.-Mexico-Canada Agreement.[31]

In the meantime, the IPEC and the NTIA should support federal legislation requiring registrars and registry operators to continue providing lawful access to WHOIS data. Such access requirements could be included in stand-alone legislation or as part of a broader privacy bill. As the NTIA and other domestic and foreign governmental entities continue to work with stakeholders and European officials, such legislation would set a baseline level of access and exercise the federal government's prerogatives regarding the application of WHOIS and privacy policy to activity with a U.S. nexus.

---

legitimate purposes that are critical to the ongoing stability and security of the Internet."), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61; Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherine Chalaby, Chair, ICANN Board of Directors (Apr. 16, 2018) (requesting an investigation into GoDaddy's throttling of Port 43 access and masking of WHOIS information), https://www.ntia.doc.gov/files/ntia/publications/redl_to_icann_on_registrar_issues_april_2018_1.pdf. *See also* Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, IGF-USA (July 27, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-igf-usa-2018; Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 63 (Oct. 22, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-63.

[29]*See* Heather Forrest, Generic Names Supporting Organization Council Chair, *GNSO Council Launches EPDP on the Temporary Specification for gTLD Registration Data*, ICANN BLOG (July 19, 2018) (discussing launch of a "fast track" policy development process to be completed by May 25, 2019), https://www.icann.org/news/blog/gnso-council-launches-edpd-on-the-temporary-specification-for-gtld-registration-data.

[30]Göran Marby, ICANN President and CEO, *ICANN GDPR and Data Protection/Privacy Update*, ICANN (Sept. 24, 2018), https://www.icann.org/news/blog/icann-gdpr-and-data-protection-privacy-update.

[31]United States-Mexico-Canada Agreement, art. 20.C.11(1)(b) (requiring each nation, in connection with the management of its country-code top-level domain, to provide online public access to a database of domain name registrant contact information, subject to each nation's law and, if applicable, relevant privacy and data protection policies), https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/20%20Intellectual%20Property.pdf.

With the dissolution[32] of the Affirmation of Commitments between ICANN and the Department of Commerce,[33] ICANN is no longer subject to a federal contractual obligation to ensure WHOIS data remains publicly accessible. And while ICANN's bylaws and policies do still include commitments to make WHOIS data accessible,[34] that, alone, has not prevented domain name registrars and registry operators from limiting WHOIS access in the face of litigation uncertainty stemming from the GDPR and ICANN's vague and overbroad Temporary Specification. Creating a clear, countervailing obligation for registrars and registry operators to provide access to WHOIS data will remove the uncertainty stemming from an overbroad application of the GDPR, and facilitate the legitimate WHOIS interests of third parties, law enforcement, and other entities. Indeed, the GDPR itself specifically allows for disclosure of data to the extent required by local law.[35]

B. The IPEC Should Push for Trade Agreements That Raise the International Level of Copyright Protection and Enforcement, Reduce Market Barriers to U.S. Movies and Television Programming, and Refrain From Expanding Online Immunities

Strong intellectual property policy is a core trade issue. Indeed, more than half of what is commonly called the U.S. "digital trade surplus"[36] comes from IP royalties and licensing fees.[37]

---

[32]*See* Letter from Lawrence E. Strickling, Assistant Secretary for Communication and Information, to Dr. Stephen D. Crocker, Chair, ICANN Board of Directors (Jan. 6, 2017), https://www.icann.org/en/system/files/correspondence/strickling-to-crocker-06jan17-en.pdf.

[33]Affirmation of Commitments Between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers, ¶ 9.3.1 (Sept. 30, 2009) (committing "to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information"), https://www.ntia.doc.gov/node/524.

[34]*See* Bylaws for Internet Corporation for Assigned Names and Numbers, art. 1, § 4.6(e)(i), (e)(ii) (as amended June 18, 2018) (stating that "subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data" and that ICANN "shall cause a periodic review to assess the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data"), https://www.icann.org/resources/pages/governance/bylaws-en; Göran Marby, ICANN President and CEO, *Data Protection and Privacy Update—Plans for the New Year,* ICANN Blog (Dec. 21, 2017) (making "it a high priority to find a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible"), https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year.

[35]*See* General Data Protection Regulation, art. 6(1)(c), 3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (allowing disclosure "for compliance with a legal obligation to which the controller is subject.").

[36]*See* Letter from Michael Beckerman, CEO, The Internet Association, to Ambassador Robert Lighthizer, U.S. Trade Representative (May 16, 2017) (touting the United States' $159 billion "digital trade surplus"), https://cdn1.internetassociation.org/wp-content/uploads/2017/05/Lighthizer-Letter-5.16.pdf.

[37]Alexis N. Grimm, Department of Commerce, Bureau of Economic Affairs, Trends in U.S. Trade in Information and Communications Technology (ICT) Services and in ICT-Enabled Services (May 2016), https://www.bea.gov/scb/pdf/2016/05%20May/0516_trends_%20in_us_trade_in_ict_serivces2.pdf.

The licensing of intellectual property, which includes copyrighted content, accounted for $124.5 billion of a total $403 billion in information and communication technology-enabled services exports—or 31 percent—in 2016.[38] Copyright and the demand for high-quality content drive global digital trade, and our trade policy should reflect this reality.

The core copyright industries of the United States—those industries whose primary purpose is to create, produce, distribute, or exhibit copyright materials—contribute more than $1.2 trillion to U.S. GDP, or close to 7 percent of the U.S. economy.[39] In terms of jobs, the core copyright industries employ more than 5.5 million workers, representing more than 4.5 percent of the U.S. private workforce, with an average annual salary of $93,221, which is 38 percent higher than the average U.S. wage.[40] The core copyright industries also outpace the rest of the economy in terms of growth, with an aggregate annual growth rate from 2012 to 2015 of almost 5 percent, more than twice the growth rate of the entire U.S. economy during that period.[41] And the copyright industries also shine when it comes to foreign sales and exports. The recorded music, motion pictures, television, software publishing, and non-software publishing copyright industries (such as newspapers, books, and periodicals) collectively represent $177 billion in overseas sales, more than the respective sales of each of the chemicals, aerospace products and parts, agricultural products, and pharmaceuticals and medicines industries.[42]

The American motion picture and television production industry remains one of the most highly competitive in the world. Approximately 450 lawful services around the globe offer audiovisual content to audiences online,[43] and the number of subscriptions to online video services around the world increased to 446.8 million in 2017—a 33 percent increase compared to 2016.[44] Contractual freedom to license on a territorial basis, a foundational copyright principle, is of paramount importance to the audiovisual sector and a driver of our sector's services trade surplus. Indeed, the U.S. entertainment industry generates $16.5 billion in audiovisual exports, registering a positive balance of trade in nearly every country in the world with a 4-to-1 export-to-import ratio, and producing a positive services trade surplus of $12.2 billion, or five percent of the total U.S. private sector trade surplus in services—larger than each

---

[38] JESSICA R. NICHOLSON, U.S. DEPARTMENT OF COMMERCE, ECONOMICS AND STATISTICS ADMINISTRATION, OFFICE OF THE CHIEF ECONOMIST, DIGITAL TRADE IN NORTH AMERICA, ESA ISSUE BRIEF #01-18, at 4 (Jan. 5, 2018), https://www.commerce.gov/sites/default/files/media/files/2018/digital-trade-in-north-america.pdf.

[39] STEVEN E. SIWEK, INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE, COPYRIGHT INDUSTRIES IN THE U.S. ECONOMY: THE 2016 REPORT 2 (2016), http://www.iipawebsite.com/copyright_us_economy.html.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] MPAA database.

[44] MPAA, THEME Report 3 (2017), https://www.mpaa.org/wp-content/uploads/2018/04/MPAA-THEME-Report-2017_Final.pdf.

of the surpluses in the advertising, mining, telecommunications, legal, information, and health related services sectors.[45]

Every indication is that the industry's trade surplus will continue to grow under expanded, legitimate, digital trade. The most significant impediment to this growth is online copyright infringement. In 2016, there were an estimated 5.4 billion downloads globally of pirated, wide-release films and primetime television and video-on-demand shows using peer-to-peer protocols—and that doesn't include other sources like streaming and downloading sites.[46] With regard to worldwide streaming piracy, in 2016 there were an estimated 21.4 billion total visits to streaming piracy sites across both desktops and mobile devices.[47] This infringement harms content creators; the platforms that license high-value, high-quality content; and the consumers who are put at risk for malware, identity theft, and fraud when they visit infringing websites. More broadly, online theft harms the health and sustainability of the online ecosystem and has a serious distorting effect on U.S. competitiveness and legitimate digital trade.

Consequently, our trade agreements should be supporting our copyright industries—and thus our economy—by including strong IP chapters, including robust civil and criminal enforcement measures. Indeed, the U.S. International Trade Commission has noted the importance of strong protections against digital piracy for U.S. creative exports.[48] A key issue in this regard is ensuring future trade agreements explicitly require the threat of civil liability for "secondary infringement," *i.e.* for businesses built around inducing or materially contributing to infringement or directly benefitting from infringement they are in a position to control. Such principles of secondary liability are well-established in U.S. law and form a critical foundation for effective online enforcement. To date, this concept has been implicit in trade agreements, but has not been realized in practice. Moreover, rightsholders should have fully effective injunctive relief, akin to that provided by Rule 65 of the U.S. Code of Civil Procedure. Future agreements should also provide for effective, deterrent criminal enforcement against commercial-scale infringement without proof of profit motive; ensure deterrent-level pre-established damages, require aiding and abetting liability for all criminal copyright offenses, and ensure camcording is a crime.

Strong provisions against circumvention of technological protection measures are also important. As discussed in Part II, above, the U.S. film and television industry relies on technological protection measures to enable diverse business models for digital content delivery.

---

[45]MPAA, THE ECONOMIC CONTRIBUTION OF THE MOTION PICTURE & TELEVISION INDUSTRY TO THE UNITED STATES (NOV. 2017), https://www.mpaa.org/wp-content/uploads/2018/03/MPAA-Industry-Economic-ContributionFactsheet_2016-FINAL-2.pdf.

[46]Alliance for Creativity and Entertainment, *The Threat of Online Piracy*, https://alliance4creativity.com/mission/the-threat-of-online-piracy/ (last visited Nov. 13, 2018).

[47]*Id.*

[48]U.S. INTERNATIONAL TRADE COMMISSION, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, PART 1 (July 2013), https://www.usitc.gov/publications/332/pub4415.pdf.

The global minimum standards for copyright in the digital environment, including legal protections for technological protection measures, are established by the World Intellectual Property Organization Internet Treaties. The IPEC should work with its interagency colleagues to ensure that our trade agreements obligate trading partners to fully and effectively implement these digital trade-enabling treaties.

Future trade agreements should avoid, however, a rote recitation of Section 512 of the Copyright Act.[49] Section 512 reflects an intent to foster a system of shared responsibility between copyright owners and service providers to deal with the problem of widespread infringement occurring over the internet. In a number of important areas that delineate this shared responsibility, however, the courts have strayed from the text and intent of the language and the overall purposes underlying section 512, to the detriment of content holders and the balance that Congress sought to strike. Moreover, we have in recent years seen other countries more effectively and nimbly respond to online piracy in their markets through site blocking, notice-and-stay-down, and injunctive relief. As such, we recommend moving to high-level language that establishes intermediary liability and appropriate limitations on liability while accommodating effective enforcement innovations made by some of our trade partners. This would be fully consistent with U.S. law and avoid the same misinterpretations by policymakers and courts overseas.

Access to foreign markets is also critically important. The nature of the online marketplace—including essentially unlimited capacity, immense diversity, and rapid change—ensures the availability of diverse content for every audience, leaving no excuse for protectionism. The IPEC should thus work with its interagency colleagues to preserve a rigorous policy of non-discrimination in the online and offline marketplace. Quotas and other discriminatory measures have no place in trade agreements.

Because copyright is such a strong contributor to the U.S. economy and trade, the last thing we should be doing is weakening copyright abroad. We thus ask the IPEC to counsel its counterparts in the U.S. government against exporting outdated limits on online liability, especially in light of domestic conversations questioning the fitness of online liability limitations at home. Poorly constructed limits on online liability may come at the expense of consumer protection, numerous public policy objectives such as curbing sex trafficking, and the copyright industries, which produce millions of jobs and a trade surplus.

Advocates for inclusion of such online liability limits—the same groups seeking to use trade agreements to weaken IP policy—are cynically transparent in stating that they wish to do so to prevent the recent efforts by Congress to re-examine them in the United States.[50] Exporting

[49] 17 U.S.C. § 512.

[50] *See* Jeremy Malcolm, Electronic Frontier Foundation, *Could Platform Safe Harbors Save the NAFTA Talks?* (Jan. 23, 2018) (arguing that one reason to include Section 230 of the Communications Act in NAFTA is to prevent Congress from modifying it in U.S. law), https://www.eff.org/deeplinks/2018/01/platform-safe-harbors-touted-safe-

these limitations for online platforms would hinder the goals of promoting the free flow of information and strengthening the global marketplace for American digital products and services. Consumers globally will be more reluctant to engage in internet communication and commerce in the face of increased online criminality, and U.S. creative industries will be hampered in their ability to export content in the face of a weakened international IP environment. The NTIA has observed that "at least one-third of online households have been deterred from certain forms of online activity, such as financial transactions, due to privacy and security concerns."[51] Online lawlessness is thus one of the more significant and growing threats to the global free flow of information online. Magnified on a global scale, these concerns can pose a real risk to U.S. economic interests at home and abroad.

Similarly, trade agreements should not include expanded articles on copyright exceptions and limitations, but instead should include a clean recitation of the three-step test, providing both rightsholders and users a familiar and widely understood and accepted framework for exceptions and limitations to copyright. The three-step test, which is the time-tested standard reflected in TRIPS, the Berne Convention, and the 1996 WIPO Internet Treaties, remains a flexible and broadly supported mechanism that supports appropriate exceptions, including in the digital environment.

C. The IPEC Should Encourage Additional Efforts by the DOJ, Immigration and Customs Enforcement, Customs and Border Protection, the FTC, the FCC, and Other Relevant Departments to Combat Piracy

Given the harms of piracy to competition and consumer welfare, we ask the IPEC to coordinate affirmative steps by the DOJ, Immigration and Customs Enforcement, Customs and Border Protection, the FTC, the FCC, and other relevant departments to combat piracy.

A critical component in the battle against piracy is enforcement by government agencies, which has significant deterrent value. A prime example is the U.S. government's 2012 criminal enforcement action against Megaupload. Then the largest piracy "cyberlocker," Megaupload alone accounted for 4 percent of all global internet traffic. The enforcement action prompted many other pirate operations to shutter. A peer-reviewed study of this reduction in piracy sources demonstrated a 6.5 to 8.5 percent increase in legitimate digital sales for three major studios in 12 countries.[52] We would expect similar beneficial results for the studios and other creators were the U.S. government to become more active in the fight against streaming, for example.

---

nafta-talks; Neil Turkewitz, *What the EFF?* (Jan. 27, 2018) (noting that the EFF has previously opposed such "policy laundering" as an inappropriate use of trade agreements), https://medium.com/@nturkewitz_56674/what-the-eff-d16950bf0a0f.

[51]Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01, *Notice and Request for Public Comments*, 83 Fed. Reg. 48600, 48600 (Sept. 26, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-09-26/pdf/2018-20941.pdf.

[52]BRETT DANAHER AND MICHAEL D. SMITH, GONE IN 60 SECONDS: THE IMPACT OF THE MEGAUPLOAD SHUTDOWN ON MOVIE SALES 4 (Sept. 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229349.

To that end, a coalition of the content community met with the National Intellectual Property Rights Coordination Center, which brings together 23 U.S. and foreign agencies under the stewardship of the U.S. Immigration and Customs Enforcement's Homeland Security Investigations division, to urge the federal government to bring criminal enforcement actions against purveyors of streaming piracy services. The IPEC also convened stakeholders and federal agencies to discuss the issue, and the MPAA would welcome the IPEC's encouragement to the DOJ to move forward with criminal enforcement actions. While DOJ pursues such criminal enforcement under current law, the MPAA also asks the IPEC to support DOJ's repeated calls for legislation closing the streaming piracy loophole.[53] In yet another example of technology outpacing the law, unauthorized distribution of copyrighted content through downloads can be prosecuted as a felony, but unauthorized streaming can be pursued only as a misdemeanor. With illicit streaming now overtaking downloading as a method of piracy, that distinction not only makes little sense, it may actually incentivize illicit enterprises to move toward streaming.

The MPAA would also welcome the IPEC's consulting with Customs and Border Protection about interdiction of illicit streaming devices entering the country from abroad, as well as coordination with other departments to bring about effective action. For example, FTC Chairman Simons attended the streaming piracy meeting the IPEC convened, and the MPAA would welcome the IPEC's recommendation that the FTC help mitigate the harm to consumers and competition that comes from piracy and the spread of malware. To date, FTC efforts appear to have been largely confined to a consumer advisory.[54] Taking more affirmative steps would help prevent unlawful services from stifling investment in, and competition by, legitimate online content services; would help combat cybersecurity threats; and would help protect consumers from identity theft and fraud stemming from malware. For example, the FTC could consider an unfair and deceptive trade practices action against entities marketing streaming piracy devices and applications as "100 percent legal" and a way to "never pay for content again," or for harm to consumers stemming from malware. An expanded effort to educate consumers and policymakers about the harms of piracy, the threat to the competitive market for American digital products and services, and the risks to cybersecurity could also pay dividends.

Lastly, one result of the IPEC meeting was a letter from FCC Commissioner Michael O'Rielly encouraging Amazon and eBay to work with the FCC to keep streaming piracy devices off their online marketplaces,[55] which they graciously agreed to do. This also opens up the possibility of FCC enforcement actions to the extent that those devices are not in compliance with

---

[53]See, e.g., 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, http://judiciary.house.gov/_cache/files/c2cf069f-5e3d-4449-8614-c05b183fd910/bitkower-doj-remedies-testimony.pdf.

[54]*See* Will Maxson, Assistant Director, Division of Marketing Practices, FTC, *Free movies, costly malware*, CONSUMER INFORMATION BLOG (April 12, 2017), https://www.consumer.ftc.gov/blog/2017/04/free-movies-costly-malware.

[55]Letter from FCC Commissioner Michael O'Rielly to Devin Wenig, CEO, President, Director, eBay and Jeff Bezos, CEO, Amazon (May 25, 2018), https://docs.fcc.gov/public/attachments/DOC-350985A1.pdf.

FCC emissions requirements and other regulations. The MPAA would welcome the IPEC's encouragement of such FCC actions.

D. The IPEC Should Encourage Internet Intermediaries to Engage in Voluntary, Collaborative Initiatives to More Proactively Curb the Mass, Unauthorized Dissemination of Copyrighted Content

A significant factor contributing to the piracy problem is a lack of accountability on the part of some online platforms—a number of which are among the world's largest internet companies—for unlawful conduct occurring over their services. While online platforms play an active and crucial, global role in providing access to content, the relationship between the platforms and the content is often seen as less direct in light of certain platforms' predominately "user-generated content" business models. Providers of curated content, by contrast, are more closely associated with the content and service environment they offer. This has led to disparate incentives when it comes to the level of responsibility assumed by large internet platforms as compared to other businesses. The lack of platform accountability presents significant risk of consumer harm and restraint on competition by unfairly forcing legitimate content production and distribution businesses to compete with material that is stolen, generally impairing the legitimate online marketplace with lawlessness, and reducing innovation and consumer choice, as people across the political spectrum are observing.[56]

The web has certainly made it easier for individuals to access and create entertainment, gather and share information, start their own businesses, conduct commerce, and interact with their government. But over the course of the last decade, we have entered an always-on, broadband and mobile, micro-targeted world where a very few, largely unregulated social media and internet platforms have massive influence over how people communicate and engage in commerce.[57]

---

[56] *See* Letter from 17 conservative organizations to Senate and House Judiciary and Commerce Committee Chairmen Chuck Grassley, Bob Goodlatte, John Thune, and Greg Walden (April 17, 2018) (stating that "many of the internet's problems result from a lack of accountability"), https://conservative.org/article/coalition-letter-expressing-support-for-recent-hearings-on-internet-platforms; Letter from 50 civil rights organizations to Senate and House Chairmen and Ranking Members John Thune, Bill Nelson, Greg Walden, and Frank Pallone (May 10, 2018) (stating that "[r]ecent events, from the 'fake news' crisis and attacks on our elections, to the widespread use of social media platforms by hate groups, have laid bare the extent of tech companies' inability—or unwillingness—to police their own platforms"), http://httponline.org/2018/05/http-joins-advocacy-groups-call-comprehensive-legislation-protect-americans-privacy-civil-rights/; Letter from 17 multicultural content organizations to Reps. Judy Chu, Mario Diaz-Balart, Michelle Lujan Grisham, and Cedric Richmond (Sept. 4, 2018) (stating that "the lack of accountability for dominant internet platforms causes serious harms and undermines trust online"), https://www.icontalks.com/wp-content/uploads/2018/09/Multicultural-Creators-Letter-9.4.18.pdf.

[57] *See* Zeynep Tufekci, *It's the (Democracy-Poisoning) Golden Age of Free Speech*, WIRED, Jan. 16, 2018 (stating that "[i]n the 21st century, the capacity to spread ideas and reach an audience is no longer limited by access to expensive, centralized broadcasting infrastructure. It's limited instead by one's ability to garner and distribute attention. And right now, the flow of the world's attention is structured, to a vast and overwhelming degree, by just a few digital platforms: Facebook, Google (which owns YouTube), and, to a lesser extent, Twitter.'"), https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship.

Unfortunately, those platforms don't amplify only the actions of well-meaning people using the internet for good. They also amplify the actions of bad actors who exploit the capabilities and reach of these platforms, often precisely as designed, as part of commercial-scale illicit enterprises.

Ordinarily, businesses are held legally accountable if they don't take reasonable steps to combat illegal activity related to their services.[58] Online platforms, however, are largely absolved from such accountability, stemming in large part from liability limits enacted by Congress two decades ago when the commercial internet was relatively nascent.[59] The presumption underlying the liability limits was that the platforms would take voluntary steps to curb abuses, but that has not happened to a sufficient degree.

Online enforcement efforts are complicated when intermediaries fail to take adequate steps to ensure their services are not being used to facilitate copyright infringement, a problem compounded by the fact that most website operators operate anonymously and outside the boundaries of the law. All stakeholders in the internet ecosystem—including hosting providers, cloud and anonymizing services, advertising networks, payment processors, social networks, and search engines—should actively seek to reduce online content theft. As MPAA Chairman and CEO Charles Rivkin observed in recent letters to Congress and in remarks before the Technology Policy Institute, more effective voluntary efforts by online platforms to curb abuse of their services—in collaboration with those impacted by the abuses—could help preserve trust online and a healthy and vibrant internet ecosystem.[60] For example:

---

[58] *See* Chairman Bob Goodlatte, *Facebook, Google and Twitter: Examining the Content Filtering Practices of Social Media Giants*, BEFORE THE H. COMM. ON THE JUDICIARY, 115th Cong. (July 17, 2018) (observing that hotels can be held liable if they don't do enough to curb sex trafficking in their rooms; nightclubs can be held liable if they don't do enough to curb drug transactions on their dance floors; landowners can be held liable if they don't do enough to protect people from hazards on their property; pawn shops can be held liable if they don't do enough to curb fencing of stolen goods in their stores; and traditional media companies can be held liable if they disseminate defamatory material, even if produced by others), https://judiciary.house.gov/hearing/facebook-google-and-twitter-examining-the-content-filtering-practices-of-social-media-giants/.

[59] *See* 47 U.S.C. § 230 (added to the Communications Act of 1934 by the Communications Decency Act, which was itself part of the Telecommunications Act of 1996, Pub. L. No. 104-104, sec. 509, 110 Stat. 56, 133, 137, available at https://www.gpo.gov/fdsys/pkg/PLAW-104publ104/pdf/PLAW-104publ104.pdf); 17 U.S.C. § 512 (added to the Copyright Act in 1998 by the Digital Millennium Copyright Act, Pub. L. No. 105-304, sec. 202(a), 112 Stat. 2860, 2877, available at https://www.copyright.gov/legislation/pl105-304.pdf).

[60] *See* Letter from MPAA CEO Charles Rivkin to House Energy and Commerce Committee Chairman Greg Walden and Ranking Member Frank Pallone (April 10, 2018), https://www.mpaa.org/policy-statement/mpaa-house-letter-online-accountability/; Letter from MPAA CEO Charles Rivkin to Senate Judiciary and Commerce Committee Chairmen and Ranking Members Chuck Grassley, John Thune, Dianne Feinstein and Bill Nelson (April 10, 2018), https://www.mpaa.org/wp-content/uploads/2018/04/180410-MPAA-FB-hearing-Senate-letter.pdf; Charles Rivkin, Chairman and CEO, MPAA, *A Declaration of Accountability for Cyberspace*, Keynote Address at the Technology Policy Institute Aspen Forum (Aug. 20, 2018), https://www.mpaa.org/speeches_and_op_eds/a-declaration-of-accountability-for-cyberspace/.

- Advertisers, advertising agencies, and online ad networks are working with stakeholders to combat fraudulent digital advertising traffic and to make sure internet ads don't inadvertently support web sites facilitating malware, piracy, and counterfeit goods.[61]

- Payment processors such as MasterCard, Visa, and PayPal are working with content creators and others to prevent websites from using those companies' financial networks to collect subscription or other revenue from unlawful online activities.

- Donuts and Radix, major operators of new domain name extensions such as .movie and .online, have a streamlined process to respond to notices from content companies and, in some cases, suspend the domain names of large-scale pirate sites registered in their domain extensions for violating their anti-abuse policies.[62]

- Amazon and eBay are working to prevent the sale over their online marketplaces of streaming devices and applications designed and marketed for piracy. Amazon has also been a strong partner in efforts to target such piracy at the source, including joint litigation and criminal referrals made against suppliers of piracy-targeted devices, and actions to significantly disrupt the unlawful applications underlying such devices.

These are all positive developments. Other platforms and internet intermediaries would do well to better emulate these types of voluntary, collaborative initiatives to combat copyright infringement and other unlawful online behavior. Unfortunately, many continue to fall short. The IPEC could do much to promote greater collaboration aimed at reducing these harms by endorsing voluntary initiatives, as it has in the past.[63] For example, more online intermediaries should adopt "trusted notifier" programs, under which they accept referrals from the content community about entities using the intermediaries' services in the aid of piracy and, after doing their own due diligence, take remedial action. In particular:

> Domain name registrars and registry operators should agree to keep WHOIS data public, to the extent permitted by law; to suspend the domain names of referred sites; to freeze the domain name so it becomes unavailable to others; and to disclose the true name and address of pirate site operators, prevent that operator from re-registering, and agree not to challenge third-party application of court orders regarding domain name suspension in cases by rightsholders against pirate sites.

---

[61] *See* Trustworthy Accountability Group, https://www.tagtoday.net/.

[62] *See* Donuts and MPAA establish new partnership to reduce online piracy (Feb. 9, 2016), https://www.mpaa.org/press/donuts-and-mpaa-establish-new-partnership-to-reduce-online-piracy/; Radix and the MPAA Establish New Partnership to Reduce Online Piracy (May 13, 2016), https://www.mpaa.org/wp-content/uploads/2016/05/Radix-and-the-MPAA-Establish-New-Partnership-to-Reduce-Online-Piracy.pdf.

[63] U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 6-7 (June 2013), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf, U.S. JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT: FY 2017-2019, at 11 (Dec. 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/2016jointstrategicplan.pdf.

Hosting providers should filter using automated content recognition technology; forward DMCA notices to users, terminate repeat infringers after receipt of a reasonable number of notices, and prevent re-registration by terminated users; implement download bandwidth or frequency limitations to prevent high volume traffic for particular files; agree not to challenge third party application of court orders regarding suspension of hosting services in cases by rightsholders against pirate sites; remove files expeditiously; and block referral traffic from known piracy sites.

Reverse proxy servers should disclose the true hosting location of pirate sites upon referral; terminate identified pirate sites, and prevent these sites from re-registering; and agree not to challenge third party application of court orders regarding suspension of reverse proxy services in cases by rightsholders against pirate sites.

ISPs should forward Digital Millennium Copyright Act notices to users; terminate repeat infringers after receipt of a reasonable number of notices and prevent re-registration by infringers; expeditiously comply with document subpoenas for user information; and block sites subject to court order in the applicable jurisdiction.

Social media should remove ads, links, and pages dedicated to the promotion of piracy devices and terminate repeat infringers.

Some argue there is tension between curbing illegal activity online and free expression. The argument is made far too broadly. Combating unlawful conduct like identity theft, unauthorized distribution of entire copyrighted works, cyberattacks, and illicit sale of opioids is no more a threat to free expression on the internet than it is in the physical world. In fact, curbing illegal activity *promotes* free expression by creating a safer environment where individuals feel comfortable to communicate and engage in commerce, and to create and lawfully access content.

Conclusion

Respect for copyright drives not just creativity, but also innovation, economic growth, and American competitiveness. Piracy—and online lawlessness generally—undermines the ability of audiences, businesses, and our nation to reap the full benefits of the internet for commerce and communication, as well as puts consumers at risk. The MPAA therefore asks the IPEC to:

- work with the NTIA and the State Department through diplomatic channels to restore and preserve access to WHOIS data;
- push for trade agreements that raise the international level of copyright protection and enforcement, that reduce market barriers to U.S. movies and television programming, and that refrain from expanding online immunities;
- encourage additional efforts by the DOJ, Immigration and Customs Enforcement, Customs and Border Protection, the FTC, the FCC and other departments to combat piracy; and
- continue encouraging internet intermediaries to engage in voluntary, collaborative initiatives to proactively curb the mass, unauthorized distribution of copyrighted content.