Before the
U.S. Department of Homeland Security
Washington, D.C. 20528

In the Matter of	)	
	)	
Presidential Memorandum	)	Docket No. USCBP-2019-0021
on Combatting Trafficking	)	
in Counterfeit and Pirated Goods	)	
	)	
Request for Comment	)	

Comments of the MPAA, IFTA, CreativeFuture, SAG-AFTRA, DGA, and IATSE

Neil Fried
SVP & Senior Counsel
Motion Picture Association of America
1600 I Street NW
Washington, D.C. 20005
(202) 378-9100

Aug. 20, 2019

Table of Contents

Overview

The internet has revolutionized communication, commerce, and creativity, allowing individuals and businesses to reach each other on an unprecedented scale, as well as helping the creative community connect with audiences. To facilitate such interaction, large online platforms for user-generated content have developed, along with a host of internet intermediaries.

Unfortunately, bad actors also use these online platforms and intermediaries for illicit activity, including piracy. Indeed, the unauthorized distribution of movie and television content on physical media—including in the stream of online commerce—is now overshadowed by the unauthorized online dissemination of such content for online consumption. This online piracy harms not just the content community, but also the local and national economies. Digital piracy is estimated to be costing the United States between 30 and 70 billion dollars annually, between 230,000 and 560,000 jobs, and between 45 and 115 billion dollars in GDP. Moreover, because pirate websites increasingly infect consumers with malware, unauthorized online dissemination of movies and television programs is a growing threat to consumers and our nation's cybersecurity.

Although there are differences between counterfeiting and piracy, as well as between hard-goods piracy and online piracy, a number of measures could help mitigate all such IP infringement. The MPAA, IFTA, CreativeFuture, SAG-AFTRA, DGA, and IATSE[1] therefore welcome the DHS's request for comment regarding the presidential memorandum on counterfeit and pirated goods trafficking, in connection with the Customs and Border Protection's Aug. 21st meeting of the Commercial Customs Operations Advisory Committee.[2] We request that the final report stemming from the memorandum, and any resulting Administration action, address online piracy in addition to counterfeiting and piracy of hard goods. In particular, we ask that the Administration:

- continue urging user-generated content platforms and internet intermediaries to collaborate with the creative community on voluntary best practices to curb copyright infringement;
- encourage the Department of Justice to bring criminal actions against entities engaged in online copyright infringement;
- persist in pressing the Internet Corporation for Assigned Names and Numbers to restore access to WHOIS data—which is essential to curbing piracy and illicit online conduct

[1] See the Appendix for descriptions of the commenting parties.

[2] *See In re* Notice of Federal Advisory Committee Meeting, Docket No. USCBP-2019-0021, DHS, Customs and Border Protection, Commercial Customs Operations Advisory Committee, 84 Fed. Reg. 37904, 37905 (Aug. 2, 2019), https://www.govinfo.gov/content/pkg/FR-2019-08-02/pdf/2019-16584.pdf; Presidential Memorandum on Combating Trafficking in Counterfeit and Pirated Goods (April 3, 2019), https://www.whitehouse.gov/presidential-actions/memorandum-combating-trafficking-counterfeit-pirated-goods/.

generally, but is being hindered by an overapplication of the European Union's General Data Protection Regulation—and support legislation if ICANN fails to do so soon; and

- raise the level of copyright protection and enforcement abroad through trade negotiations.

I. Background

A. The Facilitation of Piracy Via Online Marketplaces and Internet Intermediaries

U.S. television viewers have more content choices than ever before. The number of American scripted, original series available over traditional and online sources is up from 389 in 2014 to 495 in 2018, with the number of those series originating online growing from 33 to 160.[3] The U.S. movie and television industry makes that content available not only over broadcast, cable, and satellite services, but also through 144 lawful online services available to American audiences as of 2018, up from 112 in 2014.[4]

Unfortunately, pirates have also embraced online dissemination. So while movie and television piracy via tangible media remains a nominal problem, pirates in the last few decades have shifted first from the distribution of counterfeit video tapes to DVDs and Blu-ray discs, then to peer-to-peer download sites, and now to streaming—whether through direct, unauthorized streaming from websites; through subscription services; or through the sale of connected devices loaded with applications for online-streaming of pirated content.

In the past, 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 to reach audiences through lawful services, online piracy remains a drag on American content production and innovation. Indeed, in light of the internet's global, near instantaneous reach, unauthorized dissemination online has the most significant impact on the worldwide market for U.S. movies and television programming.

Content thieves take advantage of a wide constellation of easy-to-use online technologies, usually for monetary gain, and rely on both online platforms for user generated content and other internet intermediaries to do so. The piracy services often have the look and feel of legitimacy, sometimes luring viewers who have no intent to patronize pirate operations and may not even realize they are doing so. And just as legitimate online dissemination of movie and television programming is moving toward streaming, so, too, is piracy. 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, host sites representing 36 percent, and peer-to-peer representing 27 percent.[5] In 2017, an estimated 9.4 billion pirated movies and TV

[3]FX Networks Research (2018).

[4]MPAA database.

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

shows were downloaded worldwide using peer-to-peer protocols.[6] By comparison, there were an estimated 22.9 billion visits to streaming piracy sites worldwide that year across both desktops and mobile devices.[7] In the second half of 2017, the 10 most popular streaming piracy sites globally each saw an average of 4.5 million monthly desktop visitors worldwide.[8]

An emerging global threat is piracy from illegal internet protocol television services that provide stolen telecommunication signals or channels to a global audience. This is a particularly pernicious form of online piracy, as it is easier to use than other forms that can require the installation and use of more complicated technologies and that enable viewing of select pieces of content. Illegal IP television services often offer "plug-and-play" simplicity; enable program-guide-like scrolling through an enormous list of real-world channels from across the globe; enable viewing of those channels in near real-time, with little delay from the transmission via legitimate sources; and often include access to live sporting, pay-per-view, or other events for which there is little audience once the event is over, making the harm of the piracy all the greater. The MPAA has identified more than 1,000 illegal IPTV services operating around the world. They are accessible via dedicated web portals; third-party applications; and piracy devices configured to access the services as well as individual pieces of pirated content on demand. Such devices recently experienced a surge in consumer adoption.

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

Physical Counterfeit Products. Although digital dissemination presents the most pressing threat to the U.S. movie and television industry, hard-copy piracy and counterfeiting remains a problem. The counterfeit product's high quality, including the packaging, often makes it indistinguishable from legitimate product. Counterfeit products can be purchased from websites and online sales platforms, sometimes even legitimate ones. The sales 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.

The U.S. creative community has also produced some of the most iconic brands in the world and engages in the retail and licensing of consumer products representing billions of dollars in sales. Counterfeiting of hard-goods is thus also a major problem for this aspect of the business.

---

[6] Analysis of Mark Monitor data.

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

[8] *Id*.

Peer-to-Peer Networks and BitTorrent Portals. Peer-to-peer or file-sharing networks enlist software that allows users to join "swarms" of other users distributing movie or television content. As users download pieces of the file, their computers distribute the pieces to others in the swarm. The most popular peer-to-peer software is BitTorrent. BitTorrent websites facilitate file distribution by organizing torrent files and managing the download process. BitTorrent remains popular, serving millions of torrents or tens of millions of users at any given time.

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 download 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. The principle use and purpose of these cyberlockers is to facilitate content theft. 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."[9]

By making vast amounts of infringing premium content available to the public, these sites attract huge amounts of traffic. 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.[10]

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, and the link is removed, other links may remain, enabling continued infringement since the unauthorized content itself has not been removed. Moreover, many cyberlockers and video hosting services do not respond to takedown notices in the first place. Some may even be uploading the infringing material themselves, as well as serving as file storage sites for popular streaming piracy linking sites.

---

[9] 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.

[10] *Id.*

Linking and Streaming Websites. Linking sites aggregate and organize 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, copyrighted art to advertise the content. The sites then provide links so users can access the infringing content. They largely derive their revenue from advertising and referrals.

Depending on the website, users are commonly presented with the option of downloading a copy to their computers or streaming the content in a video-on-demand format. Many streaming link sites frame or embed video players from third-party websites, reducing the number of clicks needed to get to content while keeping the user on the site to serve advertisements. Some appear to be hosting the content on servers they control to maintain continuity of infringing offerings and to avoid takedowns on third-party file-hosting sites.

Illegal Internet Protocol Television Services. Illegal IPTV services typically offer hundreds of channels unlawfully sourced from providers worldwide, often alongside unauthorized copies of movies and television series available on demand. Many of these illegal services are subscription-based and run for profit, offering monthly or yearly packages.

The technical infrastructure related to these services can be 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 resell them for a profit, further complicating investigations.

To function, illegal IPTV 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 illegal activity. Others tailor their business strategies towards illegal sites or look the other way, even when informed—becoming bad actors themselves.

Piracy Devices and Applications. A harmful ecosystem has emerged around devices and associated "add on" software designed to illicitly stream movies and television programming, although enforcement actions are having an impact. The devices, often Android-based set-top boxes, are sometimes built around Kodi open-source media software. The add-ons connect users to streams of "live" or on-demand pirated movies, television programming, and sporting events. They enable plug-and-play connection to a standard television set, thus undermining the license fees paid by distributors on which content creators depend.

Streaming devices preloaded with infringing applications can be found online and in physical marketplaces. Additionally, 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 both legitimate and specialty app repositories that direct the user to infringing add-ons and portals.

Six percent of North American broadband households—some 6.5 million homes—are accessing subscription television piracy services, according to Sandvine.[11] A rough estimate by Sandvine suggests the streaming piracy device ecosystem may be generating ill-gotten gains of $840 million per year in North America, a number that may well be understated.[12]

B. The Threat to Creators, Commerce, Consumers, and Cybersecurity

All the forms of infringement discussed above harm a broad swath of the legitimate movie and television production and distribution sectors, including content creators, skilled craftspeople earning a middle-class living in the industry, production crews, small businesses that support productions, large and independent movie and television studios, 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 to meet evolving consumer demands. The large-scale availability of pirated content makes it more difficult 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 legitimate services and siphoning financial returns that would otherwise be available to reinvest in creative content, piracy harms competition and limits the ability of content creators and distributors to offer a wider array of choices in movies, television programming, and services. It also steals significant revenue that would otherwise go to pay cast and crew, including to fund their health and retirement plans.

The content community is not the only victim of piracy. So, too, are the national and local economies. In the process of making content available online and off, the television and film industry supports 2.6 million jobs and $177 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; contributes $229 billion in sales to U.S. GDP; generates $17.2 billion in exports; and exports 2.5 times what it imports, yielding a positive balance of trade in every major market in the world and producing a $10.3 billion trade surplus—larger than each of the surpluses in the telecommunications, transportation, mining, legal, insurance, information, and health-related services sectors.[13] In addition, the industry pays $44 billion to more than 250,000 local

---

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

[12] *Id.*

[13] MPAA, THE ECONOMIC CONTRIBUTION OF THE MOTION PICTURE & TELEVISION INDUSTRY TO THE UNITED STATES (Nov. 2018), https://www.mpaa.org/wp-content/uploads/2019/03/Economic_contribution_US_infographic_Final.pdf.

businesses each year.[14] 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. The local community sees that up-front investment regardless of whether the film or TV show becomes a hit or a flop. A recent report issued by economics firm NERA Consulting on behalf of the U.S. Chamber of Commerce's Global Innovation Policy Center estimates that 26.6 billion viewings of U.S.-produced movies and 126.7 billion viewings of U.S.-produced TV episodes are pirated digitally each year, mostly from outside the United States, and that digital video piracy is costing the United States between 30 and 70 billion dollars annually, between 230,000 and 560,000 jobs, and between 45 and 115 billion dollars in GDP.[15]

Because pirate sites increasingly use content as bait to generate revenue through identity theft and malware distribution, piracy also presents a growing threat to consumers and a new vulnerability to cybersecurity. One-third of pirate sites expose users to malware, with pirate sites 28 times more likely to infect users with malware than mainstream websites, according to the Digital Citizens Alliance.[16] 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.[17]

Making matters worse, when people use streaming piracy devices and applications, they typically place the devices on the other side of the router, past the firewall or other security measures.[18] This helps usher hackers beyond the defenses of the network the device is connected to, which can result in access to anything else connected to that network; the siphoning of massive amounts of data; theft and sale of user names, passwords, credit cards, and identities; remote, third-party control of devices and applications on the network; surreptitious use of the network by someone else, such as for mining cryptocurrency and creation of a botnet; or other harms.[19] And any malware installed can continue to reside within the network even after the user removes the piracy device.[20] Troublingly, 44 percent of individuals that have a piracy device in

---

[14] *Id.*

[15] DAVID BLACKBURN, JEFFREY EISENACH, DAVID HARRISON JR., NERA CONSULTING, *on behalf of* U.S. CHAMBER OF COMMERCE, GLOBAL INNOVATION POLICY CENTER, IMPACTS OF DIGITAL VIDEO PIRACY ON THE U.S. ECONOMY (June 2019), https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf.

[16] DIGITAL CITIZENS ALLIANCE, DIGITAL BAIT 2 (Dec. 2015), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf.

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

[18] DIGITAL CITIZENS ALLIANCE, FISHING IN THE PIRACY STREAM: HOW THE DARK WEB OF ENTERTAINMENT IS EXPOSING CONSUMERS TO HARM 3, 8 (April 2019), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

[19] *Id.* at 3-5, 8, 15-20.

[20] *Id.* at 14.

their home reported experiencing malware-related problems, as compared to 7 percent for individuals who did not have such a device installed.[21]

II. Recommendations for Administration Action

The MPAA, IFTA, CreativeFuture, SAG-AFTRA, DGA, and IATSE respectfully request that: A) the DHS and the broader Administration encourage online platforms and internet intermediaries to adopt certain best practices for curbing internet-based copyright infringement and other illicit online activity; B) the DOJ bring criminal actions against entities engaged in online copyright infringement; C) the Administration help restore access to WHOIS data critical to combatting internet-based IP infringement and other illicit online activity; and D) the Administration raise the level of copyright protection and enforcement abroad through trade agreements.

A. Advancing Voluntary Initiatives Based on Best Practices for Curbing Hard-Goods and Online Piracy, Counterfeiting, and Other Illicit Online Activity

The internet has revolutionized communication, commerce, and creativity to great public benefit. The web's decentralized nature enables anyone across the globe to contribute to its architecture and content, allowing individuals and businesses to reach each other on an unprecedented scale, as well as helping the creative community connect with audiences. Large online platforms for user-generated content have developed, along with a host of internet intermediaries, to facilitate such interaction in this decentralized environment.

Unfortunately, these online platforms and intermediaries are not just connecting well-meaning people for good. Like with any tool, bad actors also use them for illicit activity, including piracy. Unlike with any tool, however, the sheer scope of the internet—along with its pervasiveness in all facets of public, personal, and economic life; the amount of sensitive data it houses and collects; the speed and distances with which it disperses information; the number of online entities involved in completing any individual transaction or communication across the web; and the difficulty in tracking down perpetrators—presents unique challenges. Further complicating matters, the same decentralization that enables the internet to offer transformative benefits also prevents any single entity from solving problems that arise.

Internet intermediaries and online platforms for user-generated content also have less incentive than other companies to curtail piracy and other illegal activity on their services in light of their engagement-based business models, the fact that they often do not have direct relationships with the providers of the content that traverses their services, and federal policies that limit their liability for the actions of their users.[22] All of this is greatly increasing and complicating the threat of intellectual property theft, as well as other illicit online activity, such

[21] *Id.* at 4, 22.

[22] *See* 17 U.S.C. § 512 (limiting online platforms' liability for copyright infringement); 47 U.S.C. § 230 (limiting online platforms' non-copyright related liability).

as identity theft, fraud, cyber-attacks, illegal sale of opioids, and human trafficking—although we certainly do not equate all those ills with piracy.

In light of the challenges described above, the content community seeks to collaborate with user-generated content platforms and internet intermediaries on voluntary initiatives aimed at curbing piracy and that create tools and remedies available to all creators. Many of these initiatives would also help mediate hard-goods counterfeiting, trademark infringement, and other illicit online conduct, since perpetrators often rely on online platforms and internet intermediaries to facilitate their activities. The Administration has played an instrumental role in encouraging such initiatives in the past.[23]

Below is a list of some of the participants in the online ecosystem that we have approached, a description of the best practices we seek, and an indication of the progress we have seen and where it is lacking. We would welcome the DHS's engagement—as well as that of the Intellectual Property Enforcement Coordinator, the Department of Justice, the Department of Commerce, and the National Economic Council—to encourage such voluntary initiatives.

1. Payment Processors

Despite the perception of piracy as a hobby conducted by teenagers in their parents' basements, the mass, unauthorized dissemination of movie and television content is typically a sophisticated operation conducted by illicit enterprises for profit. As such, the perpetrators often charge subscriptions or other fees, which they naturally would prefer to collect through a credit card or online payment network. Many such financial networks, however, have terms of service that prohibit their use in connection with illegal activity. To help Visa, MasterCard, and PayPal enforce such provisions, we flag piracy operations for them as well as provide key indicators so they can identify such operations themselves.

By denying pirate operations access to their services, Visa, Mastercard, and PayPal not only make it more difficult for them to collect money, but also remove an air of legitimacy. Pirates must instead resort to alternative collection mechanisms—such as asking users to provide a bank account number, to place a sham order through a flower shop or some other third-party vendor, or to use cryptocurrency—which might give potential users pause. This collaboration has been one of our earliest and most successful voluntary initiatives.

2. Online Advertisers

Pirate operations also seek to make money by hosting advertising on their sites. To minimize the chances that ads for household-name products and services end up on pirate sites, the content community reached out to advertisers, ad agencies, and online ad networks.

---

[23] *See* 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.

Together, they have put in place programs to help brands avoid inadvertently funding piracy.[24] These programs have reduced the advertising revenue pirate sites receive by between 48 and 61 percent, to approximately $111 million per year.[25] A new trend we are starting to notice, however, is the appearance of advertising in streaming piracy applications.

3. Online Marketplaces

Not long ago, typing a variety of select phrases into an online marketplace's search bar would produce hundreds of offers to sell streaming piracy devices. To help stem the tide, the content community reached out to Amazon, eBay, and Alibaba. Much like with payment processors, we provided these online marketplaces with key indicators for identifying streaming piracy devices, such as inclusion of language in a seller's description like "fully loaded set-top box," "never pay for cable again," and "get instant access to any movie, TV show, or sporting event for free." Much to their credit, Amazon, eBay, and Alibaba then provided additional notices on their websites indicating that offering devices for the unauthorized distribution of copyrighted content is forbidden, and began culling listings. Since Amazon, eBay, and Alibaba started taking these actions, we have seen a marked drop in the presence of these devices on their online marketplaces.

4. Internet Connected Devices

Although internet-connected devices like those provided by Roku are predominantly used for authorized content, pirates can also use them for unauthorized dissemination of movies and television shows. The content community has reached out to Roku to address the rise of piracy on private channels. Roku has invested significant resources in the development of internal programs to address piracy on its platform, including performing a technical analysis to identify pirate activity, revising its developer registration process, and creating new security practices. As a result, we have seen a significant decrease in piracy on the Roku platform.

5. Domain Name Providers

Most domain name providers have terms of service indicating that registrants may not use domain names for illegal activity. Donuts and Radix, operators of the relatively new domain name extensions ".movie" and ".online," have each established "Trusted Notifier" programs to ensure that websites using domains registered to those companies are not engaged in large-scale piracy. Under the programs, the MPAA may refer such sites to the companies. If the companies determine that such a website is engaged in illegal activity in violation of the companies' acceptable use and anti-abuse policies, the companies may act within their already established authority to put the infringing site on hold or suspend it. Unfortunately, larger domain name

[24] *See* Trustworthy Accountability Group, Fight Internet Piracy, www.tagtoday.net/piracy.

[25] *See* EARNST & YOUNG, MEASURING DIGITAL ADVERTISING REVENUE TO INFRINGING SITES (2017), https://www.tagtoday.net/hubfs/Measuring%20digital%20advertising%20revenue%20to%20infringing%20sites.pdf?t=1507150221706.

providers—such as those operating the more frequented ".com" and ".org" extensions that host a vast amount of piracy—have refused to adopt such programs.

6. Web Hosting Services

Web 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 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. 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.

7. Reverse Proxies

Reverse proxy providers interpose their own facilities between their clients' websites and the broader internet. This means their clients never need reveal their websites' IP addresses. As a result, hackers seeking to harm the clients—for example, by launching "denial of service attacks" that overload their websites—will only reach the reverse proxy provider and its defenses. Unfortunately, some reverse proxy providers also serve bad actors seeking to shield their illicit activity. This includes operators of websites that rightsholders have identified as copyright infringers thousands or even millions of times in copyright infringement notices publicly viewable on Google's Transparency Report.[26] Some reverse proxy providers will reveal the IP address of a website after-the-fact when notified by a copyright holder of a particular infringement, but will continue serving the pirates. To prevent ongoing infringement, reverse proxy providers could and should adopt repeat infringer policies to stop working altogether with entities engaged in pervasive piracy.

8. Social Media

Because social media platforms are built around the sharing of content, they are ripe for the infringing dissemination of copyrighted material. Some social media platforms have taken steps to address this. YouTube and Facebook, for example, screen video content against "fingerprint files" provided by large copyright holders and can prevent upload of matching content. This technology can be quite effective in combatting copyright infringement, and expansion of its use to include smaller copyright holders, which are currently excluded from the process, would be helpful.

Separately, some social media platforms have taken steps to remove links to piracy-related sites' stolen content, but pro-active efforts to take down unauthorized live streams of content and generic promotions of piracy pages would also be helpful.

[26] *See* Google, Transparency Report, Content delistings due to copyright, https://transparencyreport.google.com/copyright/overview?hl=en.

B. Criminal Enforcement

A critical component in the battle against piracy is criminal enforcement by the U.S. government. Although the U.S. government does not take many such actions, those they do can have a greater deterrent effect than civil suits because criminal cases bring more attention, potential asset seizure and forfeitures, and the possibility of jail time. A prime example is the U.S. government's 2012 criminal enforcement action against Megaupload. The then-largest piracy "cyberlocker," Megaupload accounted for 4 percent of global internet traffic. The enforcement action prompted many other pirate operations to shutter or go legal. A peer-reviewed study of this reduction in piracy demonstrated a 6.5 to 8.5 percent increase in legitimate digital sales for three major studios in 12 countries.[27] We would expect similar results were the U.S. government to become more active in the fight against streaming piracy.

To that end, the content community periodically meets with the National Intellectual Property Rights Coordination Center—which brings together 25 U.S. and foreign agencies under the stewardship of the U.S. Immigration and Customs Enforcement's Homeland Security Investigations division[28]—to urge the federal government to bring criminal enforcement actions against purveyors of streaming piracy services. The Intellectual Property Enforcement Coordinator also held a roundtable in May 2018 to discuss criminal enforcement and the growing use of streaming piracy devices.[29] In attendance were representatives from the movie studios, subscription television providers, broadcasters, sports leagues, the creative community, the FBI, the Department of Homeland Security, the Justice Department, the Commerce Department, the Federal Communications Commission, the Federal Trade Commission, the U.S. Trade Representative, and Congress. The creative community has pending a number of criminal referrals to DOJ regarding streaming piracy operations, with the goal of replicating the deterrent effect and protection of legitimate consumption that happened after the Megaupload action. Our hope is that the DHS and others in the Administration will encourage the DOJ to take such action.

C. Restoring Access to WHOIS Data

One development making the piracy fight even more difficult is diminished access to WHOIS data, which contains basic contact details for holders of internet domain names. WHOIS information has been publicly available since the founding of the commercial internet. Access to WHOIS data forms the basis of online transparency, security, and accountability. Such access is necessary to protect consumer privacy, ensure public safety, and promote lawful commerce.

---

[27] 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.

[28] *See* https://www.iprcenter.gov/about.

[29] *See* U.S INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, ANNUAL INTELLECTUAL PROPERTY REPORT TO CONGRESS 26 (Feb. 2019), https://www.whitehouse.gov/wp-content/uploads/2019/02/IPEC-2018-Annual-Intellectual-Property-Report-to-Congress.pdf.

Indeed, a recent DOJ cyber report states that "[t]he first step in online reconnaissance often involves use of the Internet Corporation for Assigned Names and Numbers' WHOIS database."[30]

Domain name providers have begun restricting access to WHOIS data, however, based on an overapplication of the European Union's General Data Protection Regulation. The GDPR does not apply to non-personal information;[31] and, even in the case of personal information, the regulation allows disclosure for legitimate interests such as public safety, law enforcement and investigation, enforcement of rights or a contract, fulfillment of a legal obligation, cybersecurity, and preventing fraud.[32] 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.[33] Furthermore, it applies only to information about "natural persons," and so imposes no obligation to obfuscate information about domain name registrants that are companies, businesses, or other legal entities, irrespective of the nationality or principal place of business of such entities.[34]

Domain name providers' overapplication of the GDPR is not only limiting the ability of content creators to combat piracy, but also hindering efforts by public interest groups, the private sector, cyber-security firms, federal agencies, and law enforcement authorities to thwart online-lawlessness generally—including identity theft, fraud, cyber-attacks, state-sponsored espionage, illegal sale of opioids, and human trafficking. The DHS has urged that WHOIS data remain available, especially since it is a critical tool for combatting botnets and other online threats.[35] Yet according to an analysis by two cybersecurity working groups of more than 300 survey responses, the restriction of WHOIS data is impeding attempts to investigate cyber-attacks.[36]

---

[30]DOJ, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 35 (July 2018), https://www.justice.gov/ag/page/file/1076696/download.

[31]*See* GDPR, art. 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.

[32]*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.

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

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

[35] U.S. DEPT. OF COMMERCE AND U.S. DEPT. OF HOMELAND SECURITY, A REPORT TO THE PRESIDENT ON ENHANCING THE RESILIENCE OF THE INTERNET AND COMMUNICATIONS ECOSYSTEM AGAINST BOTNETS AND OTHER AUTOMATED, DISTRIBUTED THREATS 23, 40 (May 2018), https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final/documents/eo_13800_botnet_report_-_finalv2.pdf.

[36]ANTI-PHISHING WORKING GROUP, ICANN'S TEMPORARY SPECIFICATION SURVEY (Oct. 18, 2018), (https://apwg.org/apwg-news-center/icann-whois-access/temporySpecSurvey.

In addition, a survey of 55 global law enforcement agencies by ICANN's Public Safety Working Group reveals that 98 percent found the WHOIS system aided their investigative needs before domain name providers took these steps, as compared to 33 percent after.[37] Recent reports also indicate that reduced access to WHOIS data is hindering efforts to combat terrorism.[38] The U.S. Department of Commerce has been outspoken about the importance of WHOIS information to governments, businesses, intellectual property owners, and individual internet users across the globe, and has conveyed the concern of the United States about the lack of certainty around access to WHOIS data for legitimate purposes.[39]

ICANN has been seeking to resolve the WHOIS problem for more than a year. If it fails to do so soon, Congress may need to legislate. Indeed, the Department of Commerce sent ICANN a letter April 4 stating that "[n]ow is the time to deliberately and *swiftly* create a system that allows for third parties with legitimate interests, like law enforcement, IP rights holders, and cybersecurity researchers to access non-public data critical to fulfilling their missions."[40] The letter added that the U.S. government is expecting ICANN to "achieve substantial progress, if not completion, in advance of ICANN's meeting in Montreal in November," and observed that "[w]ithout clear and meaningful progress, alternative solutions such as calls for domestic legislation will only intensify and be considered."[41]

Senate Commerce Committee Chairman Roger Wicker echoed that sentiment in a May 6th letter to the Department of Commerce, stating that "[a]bsent a meaningful resolution to these issues, Federal legislation guaranteeing access to WHOIS data may be warranted."[42] Should ICANN's efforts drag on without resolution in sight, we ask that the DHS support such legislation. The Administration should also seek robust WHOIS access requirements in future

---

[37]Laureen Kapin, FTC Counsel for International Consumer Protection & Co-Chair, ICANN Public Safety Working Group, ICANN63 GAC Plenary Meeting 8 (Oct. 23, 2018), https://gac.icann.org/presentations/icann63%20pswg.pdf.

[38]*See* Natalia Drozdiak, *EU Privacy Laws May Be Hampering Pursuit of Terrorists*, BLOOMBERG, July 7, 2019 (reporting that U.S., European, and Canadian law enforcement used WHOIS data to identify approximately 400 domains registered to terrorist group Islamic State and make arrests, and quoting Europol official Gregory Mounier's observation that "[s]ince May 2018, [Europol has had] more and more cases of investigations that are just dropped or severely delayed because we can't have direct access to WHOIS registration data information"), https://www.bloomberg.com/news/articles/2019-07-08/european-privacy-laws-may-be-hampering-those-catching-terrorists.

[39]*See, e.g.,* Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 61 (Mar. 12, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61.

[40]Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherine Chalaby, Chair, ICANN Board of Directors (April 4, 2019).

[41]*Id.*

[42]Letter from Sen. Roger Wicker, Chairman, U.S. Senate Committee on Commerce, Science, and Transportation, to David Redl, Assistant Secretary for Communications and Information, U.S. Department of Commerce (May 6, 2019).

trade agreements, perhaps expanding on language included in the U.S.-Mexico-Canada Agreement to apply to more than just a nation's country-code top-level domain.[43]

D. Raising the Level of Copyright Protection and Enforcement in Trade Negotiations

The piracy ecosystem is complex, involving a tremendous number of entities and intermediaries. Many of the players in the ecosystem are located outside the United States, effectively out of reach of U.S. law enforcement. When coupled with market access barriers by foreign governments, piracy can cause even more harm on international consumption of U.S. content than it does on domestic consumption. Moreover, many foreign markets do not adequately protect copyrights or provide effective enforcement, including private enforcement remedies for internet piracy. At the same time, some foreign jurisdictions, such as the United Kingdom, have implemented innovative enforcement tools and practices not yet undertaken in the United States.

The U.S. government should enhance its efforts to promote international cooperation in the fight against piracy. Among other things, the United States needs to update the model of copyright enforcement it advocates in overseas markets. While much of the model is sound—focusing on core aspects of copyright law and enforcement—the Administration should redouble its efforts around internet enforcement tools, including the critical concept of secondary liability, which creates a threat of liability for internet intermediaries that facilitate or profit from piracy.

Conclusion

While the internet has certainly had a positive impact on commerce, creativity, and communication, it is also used by counterfeiting and piracy operations to the detriment of intellectual property owners, the U.S. economy, and consumers. The federal government could take a variety of steps to help ensure online platforms and internet intermediaries connect consumers with lawful businesses, not intellectual property thieves or other illicit actors. Chief among those measures are:

- encouraging best practices by payment processors, online advertisers, online marketplaces, providers of internet connected devices, domain name providers, file and web hosting services, reverse proxies, and social media companies to ensure they are not facilitating piracy or other unlawful behavior;

- bringing criminal actions against illicit actors engaged in IP infringement, to deter such behavior and protect the legitimate IP marketplace;

---

[43]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.

- helping restore access to WHOIS data, which is critical to tracking down not just IP thieves, but also bad actors engaged in other illicit online activity, such as identity theft, fraud, cyber-attacks, state-sponsored espionage, illegal sale of opioids, and human trafficking; and

- enhancing through trade agreements international cooperation in the fight against piracy, with an emphasis around internet enforcement tools, including secondary liability for internet intermediaries that facilitate or profit from piracy.

We therefore ask the DHS to endorse such action in its recommendations to the Administration in response to the presidential memorandum on combatting trafficking in counterfeit and pirated goods.

Appendix: Description of Commenting Parties

The Motion Picture Association of America. The MPAA is a champion for the global film and television industry on behalf of its members—Walt Disney Studios, Netflix Studios, Paramount Pictures, Sony Pictures, Universal City Studios, and Warner Bros. Entertainment—which have produced some of the most beloved movies and television programming around the world. To learn more, visit www.mpaa.org.

The Independent Film & Television Alliance. IFTA is the trade association for the independent motion picture and television industry worldwide and is dedicated to protecting and strengthening its members' ability to finance, produce, market and distribute independent films and television programs in an ever-changing and challenging global marketplace. IFTA represents more than 140 companies in 22 countries, the majority of which are small to medium-sized U.S.-based businesses which have financed, produced and distributed many of the world's most prominent films. To learn more, visit www.ifta-online.org/.

CreativeFuture is a nonprofit coalition of more than 550 companies and organizations and more than 250,000 individuals – from film, television, music, book publishing, photography, and other creative industries. We mobilize our members to speak up about the value of creativity, the importance of copyright in protecting creativity, and the massive harm caused by the global theft of our creative works. Millions of creatives and thousands of businesses around the world depend on copyright to bring all of us countless moments of inspiration, learning, and joy. Our mission is to advocate for strong but appropriate copyright protections and to empower creatives to speak out against piracy and how it affects their ability to create and to make a living. To learn more, visit www.creativefuture.org.

The Screen Actors Guild-American Federation of Television and Radio Artists. SAG-AFTRA is the nation's largest labor union representing working media artists. SAG-AFTRA represents approximately 160,000 actors, announcers, broadcasters, journalists, dancers, DJs, news writers, news editors, program hosts, puppeteers, recording artists, singers, stunt performers, voiceover artists and other media professionals. SAG-AFTRA members are the faces and voices that entertain and inform America and the world. SAG-AFTRA collectively bargains the wages, hours, and working conditions of its members and exists to secure strong protections for media artists. To learn more, visit www.sagaftra.org/.

The Directors Guild of America. DGA is a labor organization that represents nearly 18,000 Directors and members of the directorial team, including Unit Production Managers, Assistant Directors, Associate Directors, Stage Managers, and Production Associates who work in film, television, commercials, news, sports, documentaries, and new media. On behalf of its members, the Guild negotiates agreements governing minimum compensation, benefits, and working conditions and has achieved world-class pension and health plans and residuals provisions which reflect the contributions of members and enable them to financially benefit from the reuse of their work. To learn more, visit www.dga.org/.

The International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts of the United States, Its Territories and Canada. Founded in 1893, IATSE represents 1400,000 members who work in all forms of live theater, motion picture and television production, trade shows and exhibitions, television broadcasting, and concerts as well as the equipment and construction shops that support all these areas of the entertainment industry. We represent virtually all the behind-the-scenes workers in crafts ranging from motion picture animator to theater usher. On both the International and local union levels, the motivating principle of the IATSE is to represent every worker employed in our crafts. To learn more, visit www.iatse.net.