

**Before the U.S. House of Representatives
Committee on Energy and Commerce**

Subcommittee on Communications and Technology

Hearing on:
“STELAR Review: Protecting Consumers
in an Evolving Media Marketplace”

June 4, 2019



Statement for the Record
Motion Picture Association of America, Inc.

Neil Fried
SVP & Senior Counsel
Motion Picture Association of America, Inc.
1301 K Street NW, Suite 900E
Washington, D.C. 20005
(202) 378-9100

Summary

Describing today's programming marketplace as embodying another Golden Age of television has become cliché because it's true: American viewers have never had as much compelling content to choose from. Nor have they had as many ways to view that content, whether on their televisions, computers, gaming systems, or personal devices. The MPAA's members—Walt Disney Studios, Netflix Studios, Paramount Pictures, Sony Pictures, Universal City Studios, and Warner Bros. Entertainment—work to provide audiences with television and movie content where, when, and how they want to watch it, including over broadcast, cable, satellite, wired or wireless telephony, and online services.

This vibrant content market benefits not only television and movie fans, but also the national and local economies. The investment and work that goes into producing shows and movies helps drive jobs, wages, and trade. What makes this all possible is the dual American values of respect for free speech and respect for copyright. Together, they enable content creators to tell their stories, to recoup their investments, and to reinvest in the next project. Negotiated licensing of content in the free market best ensures audiences have robust programming options. For that reason, the MPAA disfavors compulsory copyright licenses.

Despite the vitality of the television programming market, however, piracy remains a problem. Copyright infringement harms legitimate production and distribution, reducing proceeds to pour back into both businesses, stealing significant revenue from cast and crew that would otherwise fund their health plans and retirement funds, and making it harder to provide viewers a wider array of content. And just as legitimate distribution is moving toward streaming, so too is piracy, posing ever more problems for creators, as well a growing malware threat to consumers.

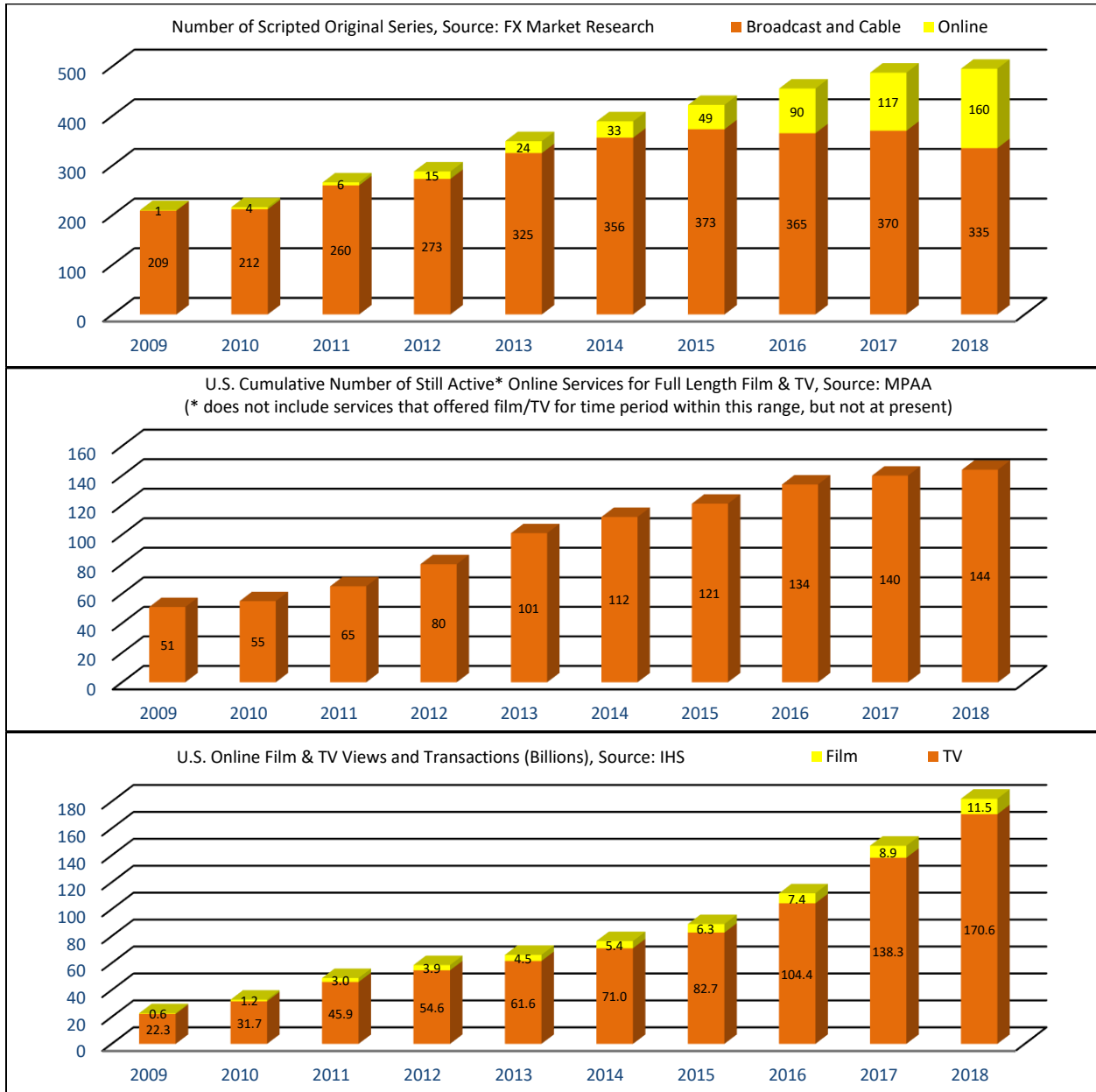
The MPAA has a three-pronged approach to combating digital piracy: 1) We look for voluntary initiatives by others in the online ecosystem to combat content thieves' illicit endeavors, and hope Congress will encourage such initiatives; 2) the MPAA's members, along with the Alliance for Creativity and Entertainment—our growing cross-industry coalition—bring civil actions against pirate enterprises; and 3) we refer cases to the DOJ for criminal enforcement against operations engaged in sufficiently significant infringement, something we hope members of the House and Senate will urge the government to pursue.

One development making the piracy fight even harder, however, is diminished access to WHOIS data, which contains basic contact details for holders of internet domain names. Domain name providers have begun restricting access to WHOIS data based on an overapplication of the European Union's General Data Protection Regulation. This is not only limiting the ability of content creators to track down pirates, but also hindering the efforts of others to thwart online lawlessness generally. The Internet Corporation for Assigned Names and Numbers has been trying to resolve the WHOIS problem for more than a year. If it fails to do so soon, Congress may need to legislate.

This industry is a success story of free expression, free markets, and intellectual property rights. Helping that success continue requires collaboration between and among private-sector actors and government to ensure the internet connects audiences with storytellers, not pirates.

The Vibrant Content Marketplace

Television viewers have more content choices than ever before. The number of 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 160.¹ The industry makes that content available not only over broadcast, cable, satellite, and telephony services, but also through 144 lawful online services available to American audiences as of 2018, up from 112 in 2014.² American viewers used those online services to access 11.5 billion movies and 170.6 billion TV episodes in 2018, up from 5.4 billion and 71 billion in 2014.³



¹FX Networks Research (2018).

²MPAA database.

³IHS Markit. See www.IHS.com.

Technological protection measures—also known as digital rights management—facilitate all this by enabling creators and distributors to offer a variety of viewing options at different prices. Because of digital rights management, audiences can choose how to access programming, including by downloading content, streaming content 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 missed episodes or to watch them all at once when a content creator makes them available *en masse*. Without technological protection measures to ensure only authorized viewers gain access to the programming, and only as authorized, content creators could not offer these choices, resulting in one-size-and-price-fits-all offerings and fewer options for viewers.

Audiences are not the only beneficiaries of this vibrant film and programming marketplace. 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.⁴ In addition, the industry pays \$44 billion to more than 250,000 local businesses each year.⁵ 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 sees that up-front investment regardless of whether the film or TV show becomes a hit or a flop.

A Product of the First Amendment and Strong Copyright Policy

Underlying this vibrant content marketplace is America’s respect for two fundamental and complementary values: free speech and intellectual property. Under the First Amendment, the speaker and the audience acting in the marketplace—not the government—determine what is said and heard. And the Constitution’s Copyright Clause recognizes that honoring the right of creators to determine how to disseminate their works increases both the production and distribution of content, to the public benefit.⁶ The ability of content producers and distributors to decide what programming to create, disseminate, and license is what makes the online marketplace so dynamic.

This respect for the First Amendment and copyright law also enables companies to manage the economic risks in the ultra-competitive video marketplace, allowing them to continue investing and innovating to deliver high-quality and diverse content to viewers. Producing and distributing

⁴MPAA, 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.

⁵*Id.*

⁶*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.”).

a major motion picture typically costs at least \$100 million, and six out of ten never recoup their initial investment. Major television productions now rival feature films not only in quality, but also in cost, sometimes reaching millions of dollars *per episode*. Yet according to one 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. Our nation’s respect for the First Amendment and intellectual property rights are very significant contributors to making America the global leader in the creation of premium content enjoyed by audiences worldwide. The best way to ensure audiences have a robust, diverse array of programming—and that creators reap the fruits of their labors to continue investing in the next story—is through negotiated licensing of content in the free market. For that reason, when it comes to the licensing marketplace for video content, it is the MPAA’s position that compulsory copyright licenses should be disfavored, and that its members are most fairly compensated through market-based negotiations consistent with copyright’s exclusive rights, and without unnecessary government intervention.

Just as a commitment to strong copyright policy in our domestic law is necessary to promote this dynamic at home, such a commitment in trade agreements is necessary to continue our market leadership abroad and to preserve the positive balance of trade. That is why the MPAA supports the copyright and intellectual property enforcement provisions of the United States-Mexico-Canada Agreement. Although the agreement should not be held out as a model for other trade pacts, it significantly improves upon the intellectual property provisions of the North American Free Trade Agreement.

Piracy, However, Continues to Present Challenges

Although the motion picture and television industry has unquestionably embraced the internet as a powerful means of reaching audiences through lawful services, online piracy remains a problem. In 2017, an estimated 542 million pirated movies and TV shows were downloaded in the United States using peer-to-peer protocols alone.⁷ And just as the legitimate marketplace is moving toward streaming, so, too, is the illegitimate marketplace. 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.⁸ Streaming device-based piracy, in particular, is a growing issue. The devices, often Android-based “set-top boxes,” are typically built around the Kodi open-source media software, but modified with illegal “add-ons.” The add-ons connect users to stored or “live” streams of pirated movies and television programming, and enable “plug and play” connection to a television. Six percent of North American broadband households—some 6.5 million homes—are accessing known subscription television piracy services, generating for pirate operations ill-gotten gains of \$840 million per year in North America, according to a report by Sandvine.⁹

⁷MarkMonitor. *See* www.markmonitor.com.

⁸Analysis of SimilarWeb data, based on sites with at least 10,000 copyright removal requests in 2017 according to the Google Transparency Report.

⁹SANDVINE, SPOTLIGHT: SUBSCRIPTION TELEVISION PIRACY 2 (Nov. 2017), <https://www.sandvine.com/hubfs/downloads/archive/2017-global-internet-phenomena-spotlight-subscription-television-piracy.pdf>.

All this infringement harms 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, movie and television studios large and small, sports leagues, broadcast and pay-TV networks and distributors, and over-the-top services. The illicit activity unlawfully competes with digital entrepreneurs and established players trying to grow lawful and innovative streaming content and distribution businesses to meet evolving consumer demands. To the extent streaming piracy diverts subscribers from legitimate services and siphons money otherwise available to re-invest, it harms competition and limits the ability of content creators and distributors to offer audiences choices in movies, television programming, and services.

Because many pirate sites disseminate malware, the spread of streaming piracy devices and applications into living rooms also presents a growing threat to consumers and a new vulnerability to cybersecurity. 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, according to the Digital Citizens Alliance.¹⁰ 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.¹¹ 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, credentials for legitimate services, 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 crypto-currency; creation of a botnet; or other harms.¹² And any malware installed can continue to reside within the network even after the user removes the piracy device.¹³ Troublingly, 44 percent of individuals that have a piracy device in their home reported experiencing malware-related problems, as compared to 7 percent for individuals who did not have such a device installed.¹⁴

Combating Piracy

The MPAA has a three-pronged approach to combating online piracy that involves: 1) voluntary initiatives by private-sector participants in the internet ecosystem; 2) civil action; and 3) criminal referrals to law enforcement.

Voluntary Initiatives. One of the internet's strengths is its distributed, interconnected nature. Because no one entity controls the web, anyone across the globe can contribute to its architecture, as well as the services and content it carries. As a result, however, no one entity can address problems that arise. Consequently, the MPAA often looks for voluntary efforts by others in the online ecosystem to join in the fight against piracy, which poses a threat to consumers and

¹⁰DIGITAL CITIZENS ALLIANCE, DIGITAL BAIT 2 (Dec. 2015), <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf>.

¹¹*Id.*, 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

¹²*Id.* at 3-5, 8, 15-20.

¹³*Id.* at 14.

¹⁴*Id.* at 4, 22.

legitimate commerce. Visa, MasterCard, and PayPal, for example, work to minimize the ability of pirate websites and sellers of streaming piracy devices to misuse those financial networks to collect subscription fees or other revenue from their unlawful pursuits. Advertisers, advertising agencies, and online ad networks have formed the Trustworthy Accountability Group to minimize the likelihood that household-name advertising inadvertently ends up on pirate websites, generating revenue for the pirates. Amazon, eBay, and Alibaba are taking steps to keep their digital marketplaces free from trafficking in streaming piracy devices. Donuts and Radix, operators of relatively new domain name extensions—such as “.movie” and “.online”—have each separately 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.

Similar initiatives by other domain name providers would be welcome. So, too, would increased efforts by video hosting services to ensure third parties are not using their platforms and storage space to peddle stolen content. And while reverse proxy services helpfully fend off denial-of-service attacks by interposing themselves between the websites of legitimate businesses and would-be hackers, the proxy services could do a better job ensuring that pirates don’t use those services to mask their true IP addresses and impede efforts to stop their theft. The proxy services should also stop doing business with repeat infringers. Some social media platforms have taken productive steps to remove piracy-related links, but pro-active efforts to take down unauthorized live streams of content, as well as generic promotions of piracy pages, would also be helpful. Congressional encouragement of these and other voluntary initiatives could help put a dent in intellectual property theft.

Civil Action. The MPAA members, along with the Alliance for Creativity and Entertainment¹⁵—a growing coalition of content producers, distributors, and online services—file civil actions against illicit enterprises engaged in piracy. Just short of two years old, ACE counts Amazon, AMC Networks, CBS, Discovery and our six studios among its more than 30 members. The alliance has already brought lawsuits in the United States that have contributed to the shuttering of three large providers of streaming piracy devices and applications: Tickbox, Dragon Box, and Setvnow.

Short of litigation, ACE also conducts “knock and talks,” which involve significant forensic work to locate key individuals involved in substantial streaming piracy operations, presenting those individuals with evidence of their illegal activity, and agreeing not to take them to court if they cease their activities and help locate others higher up in their unlawful enterprises. ACE similarly works to disrupt central, back-end elements of the streaming piracy ecosystem—such as repositories for illicit streaming applications or purveyors of unauthorized streams—to disable multiple piracy services in one fell swoop.

Criminal Referrals. The MPAA and ACE also provide evidence packages to U.S. and foreign law enforcement agencies to help those agencies bring criminal actions against sufficiently significant piracy operations. Although the U.S. government does not take many such actions, those they do

¹⁵See <https://www.alliance4creativity.com/>

can have a greater deterrent effect than civil suits because criminal cases bring more attention, along with the possibility of jail time for convicted culprits. Indeed, a 2012 U.S. action against Megaupload—then the largest piracy “cyberlocker,” accounting for 4 percent of *all* internet traffic—increased lawful digital sales by 6.5 to 8.5 percent for three major studios in 12 countries.¹⁶ The MPAA has pending a number of criminal referrals to DOJ regarding streaming piracy operations, with the goal of replicating a comparable uptick in legitimate consumption. Our hope is that Congress will encourage DOJ to move forward with those cases.

Reduced WHOIS Access Is Hurting the Fight Against Piracy and Other Online Lawlessness

One development making the piracy fight even harder 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, and is necessary to protect consumer privacy, ensure public safety, and promote lawful commerce. 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.”¹⁷

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 at all to non-personal information;¹⁸ and even in the case of personal information, the regulation acknowledges disclosure is warranted 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.¹⁹ 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.²⁰ 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.²¹

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

¹⁶BRETT 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.

¹⁷DOJ, REPORT OF THE ATTORNEY GENERAL’S CYBER DIGITAL TASK FORCE 35 (July 2018), <https://www.justice.gov/ag/page/file/1076696/download>.

¹⁸See 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>.

¹⁹See *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%20communiqué_finall.pdf.

²⁰See GDPR, arts. 2(2)(a), 3.

²¹See 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).

sector, cyber-security firms, federal agencies, and law enforcement authorities to thwart online-lawlessness generally—including identity theft, theft of intellectual property, fraud, cyber-attacks, election interference, illegal sale of opioids, and human trafficking. 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.²² 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 ICANN’s policy took effect, as compared to 33 percent after.²³ The U.S. Department of Commerce has also been outspoken about the value 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.²⁴

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.”²⁵ 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.”²⁶ Senate Commerce Committee Chairman Roger Wicker echoed that sentiment in a May 6 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.”²⁷ In keeping with this hearing’s title of “Protecting Consumers in an Evolving Media Marketplace,” restoring WHOIS access should be a priority.

Conclusion

The video content business is a success story of free expression, free markets, and intellectual property rights. Our community—the MPAA studios and the many thousands of people who work to create and make available great television shows and movies—is committed to investing and innovating to keep meeting audiences’ expectations. As the Committee considers the appropriate policies for the future of the video marketplace, we hope it will recognize that as wondrous as all the forms of distribution are, they rely on the production of content to deliver value

²²ANTI-PHISHING WORKING GROUP, ICANN’S TEMPORARY SPECIFICATION SURVEY (Oct. 18, 2018), (<https://apwg.org/apwg-news-center/icann-whois-access/temporySpecSurvey>).

²³LAUREEN 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>).

²⁴See, 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>).

²⁵Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherine Chalaby, Chair, ICANN Board of Directors (April 4, 2019).

²⁶*Id.*

²⁷Letter 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).

to consumers. Producers and creators take financial risks to make that content available. As those producers and creators continue to explore ways to distribute content, respect for copyright is necessary to help safeguard their investments from theft and illicit distribution, especially as access to stolen content becomes easier over the internet. Helping to write future chapters of the great American success story that is the television and film industry will require collaboration between and among private-sector actors and government to ensure the internet connects audiences with storytellers, not pirates.