Before the
National Telecommunications and Information Administration
Washington, D.C. 20230

In the Matter of	)	
	)	
International internet Policy Priorities	)	Docket No. 180124068-8068-01
	)	
Notice of Inquiry	)	RIN 0660-XC041

Comments of the Motion Picture Association of America

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

July 17, 2018

Table of Contents

Overview 1

I. The NTIA Should Examine Whether Decades-Old Policies Continue to Serve Their Intended Objectives and What Internet Policy Changes May Be Needed in the Modern Internet Age 3

A. The Role of the Internet in our Economy and our Culture Has Changed Dramatically Over the Past Twenty-Five Years 3

B. Connecting the Bad as Well as the Good 5

C. The Rise of Internet Exceptionalism 7

D. The Reality of Today 9

E. In Reviewing Information Policy and Advising the White House and Federal Agencies, the NTIA Should Consider Whether the Broad Privileges Afforded to Online Platforms Are Now Subverting the Aims for Which They Were Adopted . 10

F. Accountability is Not the Same as Regulation 12

G. Curbing Illicit Activity Does Not Chill Speech 12

H. The NTIA Should Support High-Standard Copyright Provisions in Trade Agreements and Advise its Government Counterparts Not to Export the Limits on Online Liability While the United States Re-examines Internet Policy 15

II. The NTIA Should Ensure ICANN, Registries, and Registrars Enforce Obligations That Prohibit Use of Domain Names in Connection with Illicit Conduct, as Well as Use Diplomatic Channels and Advise on U.S. Legislation to Ensure WHOIS Access Remains Robust 20

A. The Multistakeholder Model 20

B. WHOIS and the GDPR 22

III. The NTIA Should Help Educate Consumers and Policymakers About the Harms of Streaming Piracy Devices and Applications, and Should Encourage the U.S. Government to Bring Criminal Enforcement Actions Against Parties Promoting Piracy Through the Distribution of Such Devices and Applications 30

A. The Problem 30

B. The Impact on Legitimate Digital Commerce 31

C. The Impact on Consumers and Cyber Security 32

D. What the Private Sector is Doing to Address the Problem 33

E. The Need for Federal Government Action 35

Conclusion 36

Overview

The Motion Picture Association of America[1]—like the National Telecommunications and Information Administration—"[r]ecogniz[es] the vital importance of the internet and digital communications to U.S. innovation, prosperity, education, and civic and cultural life," and agrees it should be "a top priority to encourage growth and innovation for the internet and internet-enabled economy."[2] Toward that end, the United States has adopted a variety of policies over the past two decades aimed at promoting the development of the internet, and there is little doubt that online platforms have grown tremendously as a result. Whether and which of those policies remain fit for purpose in the modern internet era, however, is an appropriate subject of the current inquiry.

Among these policies is the decision more than 20 years ago, when the internet was truly in its infancy, to shield online platforms from responsibility for harms stemming from use of their services,[3] even though most other businesses can be held culpable for such harms in similar circumstances. That policy was then, and remains today, a significant departure from the ordinary and generally accepted rules under which firms are typically held to account for harms resulting from their services that are foreseeable and can reasonably be avoided.

In the intervening two decades, the internet has grown from a nascent platform to a central forum for social, political, and economic engagement. It has revolutionized communication, commerce, and creativity by enabling individuals and businesses to reach each other like never before.

---

[1] The MPAA is the voice of the American motion picture, home entertainment, and television industries, and represents the six major U.S. studios: Walt Disney Studios Motion Pictures, Paramount Pictures Corp., Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corp., Universal City Studios L.L.C., and Warner Bros. Entertainment Inc.

[2] NTIA International internet Policy Priorities, 83 Fed. Reg. 26036, 26036 (June 5, 2018).

[3] *See* 47 U.S.C. § 230; 18 U.S.C. § 512.

But as the internet has matured, a few online platforms have amassed an outsized influence over internet communication and commerce. Moreover, their many positive aspects are increasingly clouded by the fact that, as these platforms have become more pervasive, bad actors also are using them as powerful tools for harmful and illicit ends.

Now that the internet has reached maturity, the assumptions underlying U.S. policy—1) that in order to flourish, online platforms need to be free from the ordinary obligations borne by most businesses, and 2) that online platforms will have natural incentives to diligently and effectively curtail abuse of their services voluntarily—are rightfully coming into question.

The NTIA, as "the Executive Branch agency responsible for advising the President on telecommunications and information policy,"[4] should examine whether our decades-old approach is now having the opposite effect intended, threatening NTIA's goals of "protecting and promoting an open and interoperable internet, advocating for the free flow of information, and strengthening the global marketplace for American digital products and services."[5] It may be that continuing past policies will undermine trust in the internet as a platform; harm "the public welfare, national security, and competitiveness of the United States"; and hinder "the rapid technological advances being made in the telecommunications and information fields."[6] If an increasingly toxic online environment and a lack of accountability on the part of online platforms causes individuals, businesses, and governments to lose faith in the internet, we may see slower economic growth, increased intervention by foreign countries and entities like the European Union and the

---

4 *NTIA International internet Policy Priorities*, at 26036 (citing 47 U.S.C. § 902(b)(2)(D)).

5 *Id.*

6 *Id.* (citing 47 U.S.C. § 901(b)(1)-(6)).

International Telecommunications Union, and a retrenchment of the light-touch approach in the United States in favor of anticipatory agency regulation of online platforms.

The NTIA's solicitation of comments on its internet priorities thus arrives at an opportune moment, as the time has come for a national conversation examining whether changes in the internet ecosystem warrant adjustments to policy. We are not here advocating for any particular solution. Fostering more accountability—which is not the same as regulation—may be as simple as the platforms making good on their promise 20 years ago to effectively curb abuse of their services on a voluntary basis. But the *status quo* is clearly not working. Our hope is that proceedings like this one can begin a dialog that puts us on a better course.

As part of this conversation, the MPAA highlights three issues where the NTIA could play an important role in promoting a safe, secure, and sustainable internet:

- platform responsibility generally;
- governance of the Internet Corporation for Assigned Names and Numbers and promotion of robust, public access to WHOIS data in accordance with local law; and
- the growth of streaming piracy devices and applications.

I. The NTIA Should Examine Whether Decades-Old Policies Continue to Serve Their Intended Objectives and What Internet Policy Changes May Be Needed in the Modern Internet Age

A. The Role of the Internet in our Economy and our Culture Has Changed Dramatically Over the Past Twenty-Five Years

When the NTIA was last reauthorized, in 1992, AOL had just gone public. Google would not exist for another six years. Even by 2000, 71.1 million U.S. adults over the age of 18 were still

relying on the cacophony of dial-up modems to access the internet, representing 92 percent of those online, and 63 percent of adults 18 and over were not online at all.[7]

Since then, the internet has grown from a nascent platform to a central forum for social, political, and economic engagement. Today, the dominant online platforms are among the most powerful, sophisticated, and valuable companies in the world, and have helped revolutionize communication, commerce, and creativity to great public benefit. The web's decentralized nature enables anyone to contribute to its architecture and content, allowing individuals and businesses to connect like never before.

For the MPAA's members, that means creators and audiences have an easier time finding each other, using mechanisms and technologies that didn't previously exist. Indeed, U.S. content creators make movies and TV programming available to U.S. audiences through more than 140 legal online services, and U.S. audiences used those services to access 8.1 billion movies and 110.3 billion TV episodes in 2016 alone.[8] In the process of making content available online and off, our industry supports 2.1 million jobs across all 50 states, provides $139 billion in total wages, and contributes $134 billion in sales to the U.S. economy. [9] The industry registers a positive balance of trade in nearly every country of the world, with a 4-to-1 export-to-import ratio and a positive

---

[7] *See* JOANNA BRENNER, *FACTTANK: NEWS IN THE NUMBERS, 3% OF AMERICANS USE DIAL-UP AT HOME*, PEW RESEARCH CENTER (Aug. 21, 2013) (reporting that in June 2000, 34 percent of adults 18 and over used dial-up and 3 percent used broadband), http://www.pewresearch.org/fact-tank/2013/08/21/3-of-americans-use-dial-up-at-home/ (last visited July 13, 2018); U.S. CENSUS, TOTAL POPULATION BY AGE, RACE AND HISPANIC OR LATINO ORIGIN FOR THE UNITED STATES: 2000 (2001) (reporting 209.1 million U.S. adults 18 and over). https://www.census.gov/population/www/cen2000/briefs/phc-t9/tables/tab01.pdf.

[8] *See* MPAA, https://www.mpaa.org/what-we-do/fostering-innovation/. Underlying data on internet transactions provide by IHS Markit. *See* www.IHS.com.

[9] 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 (last visited July 13, 2018).

services trade surplus of $12.2 billion, larger than each of the surpluses in the advertising, mining, telecommunications, legal, information, and health related services sectors.[10]

This increased ability to collaborate and reach audiences has been a boon for free expression, the economy, and jobs. At the same time, the decentralized, borderless, and often anonymous nature of internet communications has subjected high-value, high-quality creative content to theft and widespread, unauthorized dissemination on a scale never before experienced. When people do not receive the well-earned fruits of their artistic and intellectual labors, creativity and independent thought suffer. That is why the mutually reinforcing traditions in the United States of intellectual property policy and respect for the First Amendment have been so critical to our nation's success. Indeed, experience demonstrates that copyright is a driver of the free flow of information. As the Supreme Court has observed, "the Framers intended copyright itself to be the engine of free expression. By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas."[11] Copyright's role as a driver of free expression applies equally online, as well as off. The incentives copyright creates are an important part of what has helped create what today is a Second Golden Age of movies and television.

B. Connecting the Bad as Well as the Good

Unfortunately, as significant as the benefits of online platforms may be, they are not just connecting well-meaning people for good. Bad actors also are using the power and reach of the platforms, and the capabilities they make commercially available, for illicit and harmful purposes, in many instances by using the platforms precisely the way they were designed. As a result, an

---

[10] *Id.*

[11] *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 558 (1985).

epidemic of harmful conduct is beginning to cast a shadow over online platforms' benefits and erode public trust. An ever-growing list of examples is fueling concerns that online platforms are facilitating harmful and even illegal behavior, including phishing and fraud, malware, cyber-espionage, identity theft and theft of intellectual property, unlawful sale of opioids and other drugs, and trafficking of minors.

In the brick-and-mortar world, such behavior is not tolerated. Businesses have a moral and often a legal obligation to act responsibly to prevent people from using their services in the aid of illicit conduct. Failure to act on those obligations can result in severe legal consequences. Under long-standing tort law doctrines—and in some cases criminal law—businesses are held accountable if they do not take reasonable steps to mitigate known or foreseeable harms from the use or misuse of their services. Recognizing that no analogy between the offline and online worlds is perfect, it is important to note that hotels that don't take sufficient steps to stop sex trafficking,[12] clubs that don't take sufficient steps to curb drug use or transactions on their dance floors,[13] pawn shops that don't take sufficient steps to prevent trafficking in stolen goods,[14] private landowners

---

[12] *See* SHEA M. RHODES, DIRECTOR, THE INSTITUTE TO ADDRESS CRIMINAL EXPLOITATION, VILLANOVA UNIVERSITY SCHOOL OF LAW, SEX TRAFFICKING AND THE HOTEL INDUSTRY: CRIMINAL AND CIVIL LIABILITY FOR HOTELS AND THEIR EMPLOYEES, https://cseinstitute.org/wp-content/uploads/2015/06/Hotel_Policy_Paper-1.pdf (last accessed July 16, 2018); WILLIAM M. SULLIVAN, ET AL., ALERT, HUMAN TRAFFICKING RAISES CORPORATE LIABILITY CONCERNS FOR THE HOSPITALITY INDUSTRY (Feb. 5, 2018), https://www.pillsburylaw.com/en/news-and-insights/human-trafficking-raises-corporate-liability-concerns-for-the-hospitality-industry.html (last visited July 16, 2018).

[13] H.R. REP. 108-66, at 68 (2003) (Conf. Rep) (explaining that "the Illicit Drug Anti-Proliferation Act ... makes it clear that anyone who knowingly and intentionally uses their property, or allows another person to use their property, for the purpose of distributing or manufacturing or using illegal drugs will be held accountable.").

[14] *See, e.g.*, 18 U.S.C. § 2314 (making it a crime to "transport[], transmit[], or transfer[] in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen."); *U.S. v. Jacobs*, 475 F.2d 270, 288 (2d Cir. 1973) (holding that someone can have "knowledge" under 18 U.S.C. § 2314 through "deliberate closing of the eyes to what would otherwise be obvious and 'reckless disregard … with a conscious purpose to avoid learning the truth.'")

that don't take sufficient steps to protect people from hazards on their property,[15] and traditional media outlets that don't take sufficient steps to avoid libel[16] can all be held accountable for the harm that results from their inaction, even though they are not the direct culprits, as House Judiciary Chairman Bob Goodlatte observed in a recent hearing.[17]

The rationale is that the responsibility for harm prevention is more appropriately borne by the businesses than the customers who might be harmed, or that the businesses should at least take a prominent role in mitigating risk. Often, businesses that serve as "platforms" for illegal activity are better situated—and have more expertise and resources—to identify potential problems and take precautionary or remedial measures. They can more readily avoid what could be catastrophic consequences for the individuals, as well as help absorb what could also be catastrophic costs. And since the businesses are profiting from the public marketing of goods and services, there is an equity in expecting them to take on certain responsibilities and act with a requisite amount of care.

C. The Rise of Internet Exceptionalism

Ordinarily, businesses are treated one of two ways: 1) regulated—like phone companies, which as common carriers are restricted in their ability to decide who to serve, to set the terms and conditions of their services, or to interfere with the content they must carry—and then granted certain immunities from liability over what their users do over their services to reflect the

---

[15] *See, e.g., Smith v. Arbaugh's Restaurant*, 469 F.2d 97 (D.C. Cir. 1973) (stating that landowners must act reasonably in maintaining their property in a reasonably safe condition in view of all the circumstances, including the likelihood of injury to others, the seriousness of the injury, and the burden of avoiding the risk).

[16] *See* W. PAGE KEETON ET. AL, PROSSER AND KEETON ON TORTS § 113, (5 ed. 1984).

[17] *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), https://judiciary.house.gov/hearing/facebook-google-and-twitter-examining-the-content-filtering-practices-of-social-media-giants/.

businesses' lack of discretion, OR 2) free from regulation, but held accountable through potential liability if they don't exercise due care for harms caused through their services.

In an effort to promote nascent electronic communication and commerce, Congress was persuaded twenty years ago to apply a different set of rules to internet platforms, granting them the best of both worlds: freedom from regulation with the ability to set their own terms and conditions, deny service to users, and exercise editorial discretion, AND protection from any real risk of liability after the fact for the harm caused on their platforms. U.S. legislators did so under notions of internet exceptionalism—the view that online platforms were so different, they must be protected from the burdens and regulatory oversight that govern the brick-and-mortar world.

This perspective was perhaps most famously expressed by Electronic Frontier Foundation co-founder John Perry Barlow in *"*A Declaration of the Independence of Cyberspace," the 1996 manifesto he penned from Davos:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> * * *
>
> You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.
>
> * * *
>
> Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our

> particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.[18]

Barlow, who recently passed away, saw the internet's better angels. He was outlining an arguably noble, grand experiment: that the virtual world be left to govern itself through its own norms and agreements—the "golden rule," rather than by the rule of law. The assumption was that the internet was capable of policing itself—that in exchange for limits on liability, intermediaries would act responsibly, voluntarily cooperate to weed out bad actors, and effectively address harmful or illegal behavior on their platforms.

D. The Reality of Today

As a tool for promoting growth of nascent internet companies, U.S. internet policies have been widely successful. But also as a result, we now have a legal framework that almost entirely insulates online platforms from accountability for all manner of harmful activities they enable. And as we are learning all too well against this backdrop, many of Barlow's assumptions were flawed.

For one, despite his assertion to the contrary, there **were** "problems among us that … need to [be] solve[d]."

Second, Barlow's whole model is dependent upon all the constituent parts of the ecosystem exercising responsibility over their particular corners of the online neighborhood. The added freedom from liability was supposed to be paired with a commitment that online platforms would themselves curb abuse of the ecosystem. Barlow himself said that "[w]here there are real conflicts,

---

[18] JOHN PERRY BARLOW, A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

where there are wrongs, we will identify them and address them by our means." But that clearly is not working. The Social Contract is in breach; the Golden Rule is under siege.

Third, the online world is not, in the end, all that different. Many of the same ills of the brick-and-mortar world are being replicated online. In many ways, those ills are not minimized by the virtual nature of the internet, but magnified by them because they are enabled at "internet scale"—globally, with very low transaction costs, to an essentially unlimited public, and often anonymously. Conduct that is unacceptable or illegal in the real world is no less unacceptable or illegal just because it has been perpetrated with digital tools, nor is it necessarily less consequential.

The reality today is that without much risk of liability for the way platforms design their services and allow them to be used, and little to no legal obligation to engage in preventative measures in exchange for the limits on liability, online platforms have much less incentive to take harm-mitigating steps common to most other businesses.

It is not surprising then that online, where there is less threat of liability, we now have a problem. The lack of accountability for product design and commercial practices, and many platforms' views that bad actors abusing their services are "not their problem to solve," are common denominators exacerbating the extent to which the list of ills is growing unchecked on the web.

E. In Reviewing Information Policy and Advising the White House and Federal Agencies, the NTIA Should Consider Whether the Broad Privileges Afforded to Online Platforms Are Now Subverting the Aims for Which They Were Adopted

As the internet matures, policymakers need to ask whether the assumptions underlying the online liability limits granted two decades ago remain valid and, in light of the growing list of abuses occurring over online platforms, whether our decades-old policies are having an effect that runs counter to what was intended. Given legal and technological developments, and the incentives

created by the platforms' business models, the balance that was sought may no longer exist, resulting in a lack of accountability.

The quid of statutory liability limitations was premised on the expected quo of online platforms acting responsibly and voluntarily to combat online abuses in an effective way. Many of the platforms are not living up to that bargain, shielded behind the broadly interpreted limits on liability that ensure few if any consequences, and failing to apply the same innovation to address internet harms that they do to other areas of their business. Many of them have also initiated litigation to broaden their liability protection, further undermining the quo.

Even Senator Wyden, one of the authors of the immunity in section 230 of the 1996 Telecommunications Act, expressed concern recently before a gathering of internet companies' executives, stating that:

> Section 230 creates the ability for the user experience that [online platforms] want to create. You've got a responsibility to use that protection to cultivate a welcoming internet. Section 230 should be a tool for weeding out the bad actors, not an excuse for somebody to go do an ostrich act. My view is that companies have a responsibility to use the tools section 230 gives the platforms. The view that platforms are nothing but neutral pipes for speech isn't going to fly in this unique time. … I've written laws to keep the old rules off your back and I did it under the idea that it was possible for technology leaders to do better. I'm concerned that your employers are now proving me wrong, and time is running out.[19]

If the platforms are not adequately fulfilling the curbing abuse "quo," they should not be getting the liability limitation "quid." The degree of their protection from lawsuits—along with the behavior it incentivizes and the accountability it diminishes—is contributing to a toxic online environment. Policymakers should revisit the old policy choices to determine why Barlow's grand experiment has seen so many failures.

---

[19] U.S. Senator Ron Wyden (D-Ore.), Introductory Remarks by Pre-recorded Video at Santa Clara University Conference: Content Moderation & Removal at Scale (Feb. 2, 2018), http://law.scu.edu/event/content-moderation-removal-at-scale/.

The content community—like all users of, and contributors to, the internet ecosystem—has an interest in seeing online platforms thrive, so that legitimate businesses can thrive along with them. For us, that better enables creators and audiences to find each other. But healthy discourse and commerce cannot happen in an unhealthy ecosystem.

Whatever differences may exist between on-line and off-line businesses, the reality of bad actors remains a constant, and virtual though the online behavior may be, the costs are real. One way or another, internet companies must exercise the level of responsibility that was originally envisioned—a level of responsibility many are not living up to today.

F. Accountability is Not the Same as Regulation

Some seek to forestall attempts at promoting greater accountability by mischaracterizing and demonizing them as regulation of the internet. But fostering more accountability could be as simple as the platforms making good on their promise 20 years ago to effectively curb abuse of their services on a voluntary basis.

In any event, applying the rule of law and holding platforms accountable—based on longstanding judicial standards—when they fail to stop illicit activity they know about or that is reasonably foreseeable, is not the same thing as regulation. It in no way resembles anticipatory rules adopted and imposed by Congress or agencies constraining the rates, terms, or conditions by which the platforms may operate. To the contrary, it is the same responsibility under which all other unregulated businesses operate.

G. Curbing Illicit Activity Does Not Chill Speech

Sometimes the platforms argue that they should not be arbiters of what makes it online. But the point of Section 230 of the Communications Act was to encourage platforms to combat abusive internet behavior in exchange for liability protection from complaints about how they do so, or whether they do so incompletely. The fiction of neutral platforms not only shirks the bargain

underlying the liability limits in section 230; it ignores that the business decisions the platforms make in designing their services influence what large swaths of the globe see. And as we have witnessed, the refusal of platforms to curb harmful and illicit behavior on their services has allowed bad actors to thrive with near impunity and is distorting public discourse.

Moreover, our focus here is not on expression protected by the First Amendment, but on illicit conduct. Combatting phishing and fraud, malware and botnets, identity theft, theft of entire movies and television shows, counterfeiting, cyber-espionage, and unlawful sale of drugs is no more a violation of free expression on the internet than it is in the physical world. Responsible businesses refusing to facilitate such activity are not squelching speech. They are not stifling speakers wishing to communicate ideas, but thwarting culprits engaged in malfeasance. In fact, curbing such illicit activity promotes free expression by creating a safer, virtual forum where individuals feel comfortable to engage and communicate. In this sense, it is leaving lawlessness and bullying unchecked that is chilling free speech.

The rebuttal is often that there is a risk that efforts to combat illicit conduct online will be overbroad, and inadvertently chill speech. But the platforms appear increasingly willing to curb things like hate speech. As odious as such speech is, it is quintessentially expressive. Efforts to combat it are fraught with challenges of under- and over-inclusiveness. Such activity is more susceptible to a chilling speech argument than attempts to curtail clearly illicit conduct, which present a brighter line.

Some argue that asking platforms to curb behavior that is unlawful in the United States is unwise because despotic regimes overseas may pressure platforms to block activity that runs afoul of their oppressive laws. But this is not a new issue, as online platforms already have policies about the extent to which they will comply with the local laws of foreign jurisdictions. There may well

be "illegitimate" laws abroad. "[R]epressive governments," the NTIA observes, are "restricting access to information that they deem to be politically or socially objectionable … by blocking certain applications, impeding the use of Virtual Private Networks (VPNs), or through the total shutdown of internet communications within national territories."[20] That does not mean, however, that we shouldn't give force online to legitimate laws, including those that "enable[] basic human rights."[21] In this instance, we are asking that online platforms work to combat conduct—such as fraud, identity theft, theft of intellectual property, sex trafficking, and illicit sale of drugs—that are universally recognized as unlawful, including in international treaties.

Regardless, online platforms are not governments, so censorship is not an accurate description of our request that online platforms do more to combat harmful and illicit activity. In fact, the platforms themselves have a First Amendment right to determine not only what to carry, but also what speech they wish not to sponsor, and have little restriction on their editorial discretion other than perhaps an obligation to be transparent, nondiscriminatory, comply with their terms of service, and be able to address complaints. The internet is and will remain an open forum. If competition is as robust and barriers to online entry as low as the platforms say, there will always be a multiplicity of online outlets (in addition to the more traditional ones) for differing viewpoints; the question is whether consumers will have responsible, reliable outlets from which to choose.

The NTIA also seeks comment on the "emerging trend of national courts issuing judgments on internet-related court cases that risk forcing American companies to globally remove information hosted online," cautioning that "what may be censored information in one country

---

[20] NTIA International internet Policy Priorities, 83 Fed. Reg. 26036, 26037 (June 5, 2018).

[21] *Id.*

could be protected speech in other countries, including in the United States."[22] While the NTIA may be correct that some "jurisdictional disputes illustrate the tension between a global, borderless internet and national sovereignty,"[23] NTIA's concerns are not founded where the scope of an order is necessary to give effect to the court's decision within its territory, with respect to parties subject to its jurisdiction, in circumstances where doing so does not offend the law of other jurisdictions and involves conduct that is widely agreed to be unlawful and subject to remedy.[24] Such cases do not raise the censorship of expression concerns articulated by the NTIA.

H. The NTIA Should Support High-Standard Copyright Provisions in Trade Agreements and Advise its Government Counterparts Not to Export the Limits on Online Liability While the United States Re-examines Internet Policy

Strong intellectual property policy is a core digital trade issue. America's IP industries are among the most successful in digital trade. Indeed, more than half of what is commonly called the U.S. "digital trade surplus"[25] comes from IP royalties and licensing fees.[26] Copyright and the demand for high-quality content drive global digital trade, and our trade policy should reflect this

---

22 *Id.*

23 *Id.*

24 *See, e.g.*, *Equustek Solutions Inc. v. Jack*, 2018 BCSC 610 (Sup. Ct. B.C. April 16, 2018) (refusing to set aside an injunction requiring Google to de-list worldwide from its internet search results certain websites that were violating previous court orders, and that were being used to infringe upon the plaintiff's intellectual property rights, on the grounds that the court was not demanding extra-jurisdictional enforcement of the injunction in U.S. courts, but merely acting "to protect the integrity of its own process through orders [it] directed to parties over whom it has personal jurisdiction," noting that there was "no suggestion that any U.S. law prohibits Google from de-indexing those websites, either in compliance with the injunction or for any other reason."), http://www.courts.gov.bc.ca/jdb-txt/sc/18/06/2018BCSC0610.htm.

25 *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.

26 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.

reality. For example, 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.[27] Online video content viewing also continued to increase in 2017, reaching 167.5 billion views and transactions—a 41 percent increase compared to 2016.[28] 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.[29] 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, which totaled $12.2 billion in 2016, or five percent of the total U.S. private sector trade surplus in services.[30]

Indeed, 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.[31] 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

---

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

[28] *Id.*

[29] 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/commerce.gov/files/media/files/2018/digital-trade-in-north-america.pdf.

[30] MPAA, THE ECONOMIC CONTRIBUTION OF THE MOTION PICTURE AND 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 (last visited July 13, 2018).

[31] 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.

than the average U.S. wage.[32] 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.[33] 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.[34]

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 NTIA to counsel its counterparts in the U.S. government against exporting in NAFTA or other trade agreements limits on online liability, especially in light of domestic conversations questioning 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 in NAFTA—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.[35]

---

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *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-

Not only is this a misuse of trade policy, but exporting these limitations for online platforms would hinder the NTIA's goal 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.

Indeed, the Federal Communications Commission observed as far back as 2010 that distrust in online safety and security was a potential deterrent to engagement online.[36] Concerns over online ills have only grown since then. 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.

Rather than weakening copyright policy, our trade agreements should be supporting our copyright industries—and thus our economy—by including strong IP chapters. Indeed, the U.S. International Trade Commission has noted the importance of strong protections against digital piracy for U.S. creative exports.[37] In addition to the IP provisions in existing U.S. free trade agreements, a key issue in this regard is ensuring future trade agreements explicitly require the

---

touted-safe-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.

[36] *See* FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 17, 52-53, 56, 168 (March 2010) (observing that "[a]lmost half of all consumers have concerns about online privacy and security, which may limit their adoption or use of broadband," that "[i]nnovation will suffer if a lack of trust exists between users and the entities with which they interact over the Internet," that "[e]nsuring growing adoption and utilization of broadband requires that Internet users feel that they can connect and interact safely online," and that among the reasons cited by 22 percent of non-broadband adopters for staying offline was that they were "'worried about all the bad things that can happen if [they] use the Internet.'"), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[37] 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.

threat of civil liability for "secondary infringement," *i.e.* for businesses built around inducing infringement or directly benefitting from infringement they could mitigate. To date, this concept has been implicit in trade agreements, and has not been realized in practice.

Strong provisions against circumvention of technological protection measures are also important. For example, MPAA member companies use encryption technology—also called technological protection measures—to prevent content from being illegitimately accessed or distributed. Such TPMs are crucial for enabling diverse business models for digital content delivery. Content creators and distributors' widespread adoption of TPMs has enabled consumers an expanded menu of options for enjoying content, including paying for a movie online and downloading it to a hard drive, streaming a movie for a limited time on a pay-per-view basis, or enjoying a film as part of a subscription service. The global minimum standards for copyright in the digital environment, including legal protections for TPMs, are established by the World Intellectual Property Organization internet treaties. The NTIA 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.

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 450 million downloads in the United States 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;

worldwide, that number climbs to 5.4 billion.[38] 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.[39] 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.

II. The NTIA Should Ensure ICANN, Registries, and Registrars Enforce Obligations That Prohibit Use of Domain Names in Connection with Illicit Conduct, as Well as Use Diplomatic Channels and Advise on U.S. Legislation to Ensure WHOIS Access Remains Robust

Two related areas in which the NTIA can promote the free flow of information globally and advance U.S. digital commerce is ICANN governance and preserving robust access to WHOIS data. Both are critical to promoting online platform responsibility and ensuring a safe, secure, and sustainable internet for commerce, communication, and creativity. We therefore welcome the NTIA's diligence, through its own auspices and as a participant in groups such as ICANN's Governmental Advisory Committee, in seeking to ensure: 1) the multistakeholder governance model remains transparent, credible and accountable, and 2) an overbroad application of the E.U.'s General Data Protection Regulation does not restrict access to WHOIS data.

A. The Multistakeholder Model

We ask the NTIA, consistent with its commitment to remain diligent after the transition of the Internet Assigned Numbers Authority functions, to continue making internet governance a top

---

[38] Alliance for Creativity and Entertainment, *The Threat of Online Piracy*, https://alliance4creativity.com/mission/the-threat-of-online-piracy/ (last visited July 17, 2018).

[39] *Id.*

policy priority. Specifically, we hope the NTIA will help ensure ICANN, registries, and registrars are enforcing obligations that prohibit domain holders from using domain names in connection with illicit conduct. Doing so is critical to ensuring the multistakeholder model maintains the security, stability, and resiliency of the internet domain name system.

As the House Energy and Commerce Committee has recognized, the multistakeholder model relies on: 1) a transparent and credible mechanism by which the public, private sector, governments, and civil society can adopt policies, contractual agreements, and best practices to govern the functioning of the internet in a manner that promotes safety, security and resiliency; and 2) respect for those policies, agreements, and practices, and a way of holding accountable parties who consistently breach them.[40] In the post-IANA transition era, that transparency, credibility, and accountability is all the more important.

It is essential that ICANN, as well as registries and registrars, comply with and enforce the contractual obligations that were created through the multistakeholder process, some dating as far back as at least 2001, that prohibit, among other things, domain registrants from using domains in connection with illegal and abusive activity, such as directly or indirectly infringing the rights of others, or posing threats to public safety. The Registrar Accreditation Agreement, Registry Agreements and related Public Interest Commitments, for example, require registrars and registries to prohibit domain name holders from using them for unlawful activity, to investigate claims of abuse, and to provide consequences for violations, including suspension of domain names in

[40] *See* H.R. Rep. 114-175, at 5 (2015) (observing in connection with passage of the Domain Openness Through Continued Oversight Matters Act of 2015 that "[f]ailure to enforce obligations created through the multistakeholder process would jeopardize the transparency, credibility, and accountability needed for the multistakeholder governance model to work and give credence to those who argue that governments, not stakeholders, must define relationships on the Internet."), https://www.congress.gov/114/crpt/hrpt175/CRPT-114hrpt175.pdf.

appropriate circumstances. These obligations were intensively negotiated for years, opened to the multistakeholder community for public comment, and approved by the ICANN board. Such obligations are the cornerstone for accountability within the multistakeholder framework. Failing to enforce these provisions jeopardizes the credibility and accountability of ICANN and the multistakeholder governance model, and invites government intervention.

Equally important is the need for transparency to ensure that the community is able to assess what ICANN is doing to monitor and enforce compliance, not just reactively, but also proactively in response to the growing body of data that indicates patterns of abusive activity and the relationship of such abuse with particular contracted parties. If ICANN believes that its agreements with contracted parties are insufficient to form a basis for action, then such agreements need to be clarified to provide ICANN with the tools it needs to reduce the level of abuse in the domain name system.

B. WHOIS and the GDPR

We ask NTIA to continue using its involvement in ICANN and other diplomatic channels to ensure WHOIS data remains readily accessible. In particular, we urge the NTIA to:

1. advise Congress on legislation that will ensure ICANN, registries, and registrars adopt and enforce policies and practices that continue the collection of accurate WHOIS data and the ready availability of such information and, to the extent such information is justifiably limited by laws of other jurisdictions, that such information can be readily accessed for legitimate purposes; and

2. work to ensure the implementation of new laws and regulations, domestically or internationally, preserves the vital functions and access to registrant data of the WHOIS service to the greatest extent possible, taking into account the privacy interests of natural persons.

Publicly accessible WHOIS data, containing identifying information about domain name registrants, has historically been a cornerstone of online accountability and supports the stability, safety, and security of the internet. From its founding, WHOIS was designed as a protocol for a

public directory to allow anyone to contact any individual who has obtained a domain name. Domain name registrants have long been on notice that they must provide certain identifying information that will be publicly disclosed, and that such information may be used for matters of public safety, consumer protection, dispute resolution, and enforcement of rights. Preserving robust access to WHOIS data is thus essential to meeting the United State's 2017 national security strategy of ensuring a "strong, defensible cyber infrastructure [that] fosters economic growth, protects our liberties, and advances our national security."[41] Indeed, as the U.S. Departments of Commerce and Homeland Security recently observed in a May 2018 report, "[d]ata-protection policies, both in the United States and internationally, should not disrupt existing tools, such as the widely used WHOIS database of domain ownership data"; "RIRs and registrars can facilitate attribution of bad actors by maintaining accurate WHOIS databases"; and "the federal government should work to engage with its European counterparts to ensure that timely access to WHOIS information is preserved as the European data privacy protections are enforced to preserve a critical tool for domestic and global efforts to investigate botnets."[42]

ICANN's responsibility to coordinate WHOIS data as part of its mission includes ensuring adequate accuracy and access for parties with legitimate interests. Yet ICANN has recently proposed a Temporary Specification that makes significant changes to the publication of WHOIS

---

[41] NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 13 (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[42] 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, 24 (May 2018), https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

data, and thereby disrupts its essential and historical purpose, under the goal of complying with the European Union's General Data Protection Regulation.[43]

Respecting the privacy rights of natural persons need not be a hindrance to effective enforcement of consumer protection and other laws. While the GDPR and similar initiatives pose challenges to data collectors and processors, we believe it is possible to balance privacy interests with effective enforcement, provided that those with legitimate interests are able to access the necessary data. Privacy should not eviscerate transparency to the detriment of internet users and other stakeholders. With the IANA transition complete, and criminal actors increasingly exploiting the online world, we need transparency in the way the internet operates more than ever before. Only then can we realize the positive vision we all have for the internet, while establishing mechanisms to prevent or hold accountable those who would use it for illicit purposes.

Unfortunately, the interim ICANN proposal takes an overbroad approach to the GDPR and removes access to basic WHOIS information, such as registrant email address, and mandates registrars and registry operators hide information such as city, leaving internet users and others with legitimate interests without direct access to such information. The GDPR and Temporary Specification took effect mid- to late May, and early experiences reveal that registrars and registry operators have largely taken an opaque and fragmented approach, which stymies IP and other enforcement efforts. Out of the 30 WHOIS requests with respect to pirate sites that the MPAA made in June directly to registrars in 14 generic top level domains (e.g., .com, .org, .net) and 16 country code top level domains (e.g., .nu, .tv), the MPAA received the relevant WHOIS data with respect to only one request. All others were either denied, refused absent a subpoena or court order,

---

[43] ICANN, TEMPORARY SPECIFICATION FOR GTLD REGISTRATION DATA (adopted May 17, 2018), https://www.icann.org/resources/pages/gtld-registration-data-specs-en.

denied with a requirement to request the data in a particular format, or obscured with a privacy proxy. Our understanding is that many other parties with legitimate interests are running into similar difficulties. Except for the data behind privacy proxies, this information would ordinarily have been public, and even in privacy proxy cases, we sometimes had agreements in place to gain access to the underlying information to address piracy issues.

Restricting access to more WHOIS data than is absolutely necessary under the GDPR will diminish online transparency, responsibility, and accountability, as well as jeopardize internet security and safety. This new framework frustrates even preliminary examinations into illicit online activity, such as identity theft, cyber-attacks, theft of intellectual property, fraud, unlawful sale of drugs, human trafficking, and other criminal behavior, as a number of U.S. and international law enforcement, private, and public sector organizations have observed.[44]

The MPAA does not suggest that registrars and registries should violate the GDPR, but the temporary specification permits registrars and registry operators to restrict access to information in a manner that goes well beyond what the GDPR requires. The GDPR does not apply at all to non-personal information; and even in the case of personal information, the European directive acknowledges legitimate interests can warrant disclosure, such as public safety, law enforcement and investigation, enforcement of rights or a contract, fulfillment of a legal obligation, cybersecurity, and preventing fraud. Moreover, the GDPR does not apply to American registrars and registries with respect to domain name registrations by U.S. registrants, or any other domain name registrants located outside the European Economic Area. Furthermore, it applies only to information about "natural persons," and so imposes no obligation to obfuscate information about

[44] *See* 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.

domain name registrants that are companies, businesses, or other legal entities, irrespective of the nationality or principal place of business of such entities. Applying any GDPR-related restrictions on the WHOIS data of domain name registrants other than natural persons that are residents of the EEA thus goes beyond the directive's scope, will interfere with law enforcement and efforts to combat illicit online activity, and may even conflict with existing federal statutes.

We know the NTIA shares many of our concerns, and we thank the NTIA for its efforts, along with others, to preserve robust access to WHOIS data. Indeed, as U.S. Assistant Secretary of Commerce for Communications and Information and NTIA Administrator David Redl said in his March 12 speech at ICANN 61 in Puerto Rico, "one of the top policy priorities for the United States in ICANN is the preservation of the WHOIS service … [T]he United States would encourage revisions to the model to permit access to the most amount of registration data as possible"; will insist that "[p]lans … 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 "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 legitimate purposes that are critical to the ongoing stability and security of the Internet."[45]

Similarly, in its March 15 ICANN 61 communiqué, ICANN's Governmental Advisory Committee, reflecting a formal consensus view of its more than 170 member countries and economies, recognized that "[t]he current WHOIS system helps achieve many such public policy interests, including enhancing trust in the DNS, ensuring consumer protection, protecting

---

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

intellectual property, combating cyber-crime, piracy and fraud, to cite but a few of the elements"; stated that the GDPR applies only to "the privacy of natural persons and allows for the processing of and access to data for legitimate purposes"; urged ICANN to "maintain, to the greatest extent possible, the current structure of the WHOIS"; cautioned against any "proposal to hide the registrant email address as this may not be proportionate in view of the significant negative impact on law enforcement, cybersecurity and rights protection"; observed that the GDPR "[d]istinguish[es] between legal and natural persons, allowing for public access to WHOIS data of legal entities"; called for "continued access to the WHOIS, including non-public data, for users with a legitimate purpose, until the time when the interim WHOIS model is fully operational"; and urged ICANN to "[c]omplete the interim model as swiftly as possible."[46]

The U.S. House of Representatives Committee on Energy and Commerce conducted significant oversight of ICANN, and generally of the domain name ecosystem, prior to the IANA transition in 2016. In that context, the Committee was repeatedly assured that ICANN would adhere to its 2009 "Affirmation of Commitments" with the U.S. Department of Commerce. In that document, ICANN committed to "enforcing its existing policy relating to WHOIS," and emphasized the importance of a WHOIS policy that "meets the legitimate needs of law enforcement and promotes consumer trust."[47]

An expectation that these commitments would be honored was a significant motivator in the decision by Congress to remove the legislative impediments to the IANA transition. Further,

---

[46] ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—San Juan, Puerto Rico* (March 15, 2018), https://gac.icann.org/advice/communiques/20180315_icann61%20gac%20communique_finall.pdf.

[47] Affirmation of Commitments by the United States Dept. of Commerce and ICANN ¶ 9.3.1 (Sept. 30, 2009), https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en.

ICANN's current bylaws require that ICANN "use commercially reasonable efforts to enforce its policies relating to registration directory services and 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."[48]

The Committee just had another hearing, this time on draft NTIA reauthorization that would emphasize the NTIA's role in preserving robust access to WHOIS data.[49] In light of Congress' continued concern with this issue, and evidence that robust, public access to WHOIS data is in jeopardy in ways that go far beyond the requirements and jurisdictional scope of the GDPR, the MPAA asks that the NTIA advise Congress regarding legislation that would require access, consistent with the statements of the NTIA and the GAC that access should continue to the greatest extent possible. With the exception of registrants who are natural persons and confirmed residents of the EEA, registries and registrars should continue to publish in a publicly accessible WHOIS directory all domain registrant data that their current contracts with ICANN (the Registrar Accreditation Agreement or the applicable Registry Agreement) requires to be collected and made public—even if doing so requires reversal of changes they have already made or are preparing to make.

Moreover, to the extent that public access to certain information is appropriately restricted, a framework is urgently needed to enable access for those with legitimate purposes, for individual

---

[48] Bylaws for Internet Corporation for Assigned Names and Numbers, Art. 1, § 4.6(e)(i) (as amended June 18, 2018), https://www.icann.org/resources/pages/governance/bylaws-en/#article1.

[49] *Discussion Draft: National Telecommunications and Information Administration Reauthorization Act of 2018*, BEFORE THE H. COMM. ON ENERGY AND COMMERCE, SUBCOMM. ON COMMUNICATIONS AND TECHNOLOGY, 115th Cong. (June 26, 2018), https://energycommerce.house.gov/hearings/discussion-draft-national-telecommunications-and-information-administration-reauthorization-act-of-2018/.

queries as well as for cross-referencing purposes to enable investigation and enforcement against abusive and illegal activity. ICANN has failed to provide such a framework.

The consensus advice from the GAC in its June ICANN 62 Panama City Communiqué states that "a unified access model is central to providing access to non-public WHOIS data for users with a legitimate purpose and this should continue to be addressed as a matter of urgency," and advises the ICANN board to "[t]ake all steps necessary to ensure the development and implementation of a unified access model that addresses accreditation, authentication, access and accountability, and applies to all contracted parties, as quickly as possible."[50] Contracted parties within the ICANN community are nonetheless resisting efforts to address this as part of the Policy Development Process that is about to get underway, and which will produce a set of rules to take the place of the Temporary Specification.

It is imperative that registrars and registries, together with others in the ICANN community (such as public safety non-governmental organizations, cyber-security professionals, and intellectual property owners), actively work in good faith and accelerate their work on creating a GDPR-compliant accreditation framework—before any WHOIS data is removed from public access—that allows qualified access for legitimate purposes to other information to the limited extent that the GDPR requires the termination of public access to such information.

---

[50] ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—Panama City*, at 7 (June 28, 2018), https://gac.icann.org/advice/communiques/public/icann62_gac_communiqué-ar.pdf.

III. The NTIA Should Help Educate Consumers and Policymakers About the Harms of Streaming Piracy Devices and Applications, and Should Encourage the U.S. Government to Bring Criminal Enforcement Actions Against Parties Promoting Piracy Through the Distribution of Such Devices and Applications

Another way the NTIA can protect and promote an open and interoperable internet, support the free flow of information, and strengthen the global marketplace for American digital products and services, is by helping combat the growing threat from piracy devices and applications that facilitate the unauthorized streaming of copyrighted content.

A. The Problem

Illicit enterprises built on theft are increasingly peddling internet-connected devices preloaded with software to illegally stream—either "live" when they are being aired or "on demand"—a nearly infinite number of pirated shows, television channels, and movies. Just as streaming is a growing method by which consumers lawfully access movie and television content, streaming piracy has now edged out illicit downloading, with streaming piracy sites representing 59 percent of online site methods for accessing unauthorized content in June 2017.[51] Preloaded streaming device piracy is a growing subset of that streaming piracy.

Pirate operations are marketing the devices through a number of common retail channels—online platforms, mall kiosks, and at trade show booths—using tag lines like "fully loaded" and "never pay another cable bill." The devices, often Android-based "set-top boxes," are typically built around the otherwise legal Kodi open-source media software, but are modified with illegal "add-ons" that provide a user-friendly interface that connects users to streams of pirated content and enable "plug and play" connection to a television. To an average consumer, the experience is not dissimilar to using a legitimate streaming product, such as an AppleTV or Roku box, except

[51] Netnames, *Piracy Trends* (2017Q2).

the content has been stolen. Web sites enable "one-click" installation of modified Kodi software onto a set-top box, smartTV, smartphone, or other internet-connected device, or alternatively allow modification of Kodi software already on a consumer's device. Preloaded devices are sold for a flat fee, typically between $50 and $300; some also require a subscription to access the underlying streaming piracy sites, which are curated and updated.

B. The Impact on Legitimate Digital Commerce

At least six percent of North American broadband households—some 6.5 million homes—now have a Kodi device configured to access pirated content.[52] This harms a broad swath of the legitimate movie and television production and distribution sectors, including content creators, unions, large and independent movie and television studios, sports leagues, broadcast and pay-TV networks and distributors, and over-the-top services, all of which have worked to develop lawful and innovative new streaming services to meet evolving consumer demands.

One rough estimate suggests that the new streaming piracy ecosystem may already be generating ill-gotten gains of $840 million per year in North America, and that number may well be understated.[53] This illicit ecosystem unlawfully competes with digital entrepreneurs and established players trying to grow lawful online content and distribution businesses. To the extent streaming piracy diverts subscribers from legitimate services and thereby siphons money otherwise available to invest in content, it harms the global marketplace for American digital products and services and hinders the free flow of information.

---

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

[53] *Id.*

C. The Impact on Consumers and Cyber Security

Because many pirate sites also disseminate malware, the spread of streaming piracy devices and applications into living rooms presents a growing threat to consumers and a new vulnerability to cybersecurity, offering another reason for the NTIA to get involved. In May 2018, the U.S. Departments of Commerce and Homeland Security issued a report that examines ways to enhance the resilience of the internet and communications ecosystem.[54] The report came in response to an Executive Order issued a year earlier that called for an "open and transparent process to identify and promote action by appropriate stakeholders" to "dramatically reduce threats perpetrated by automated and distributed attacks (*e.g.*, botnets)."[55]

The issues relating to illegal streaming sites, devices, and applications—as well as the surrounding piracy ecosystem more generally—are thus closely linked to broader issues of cybersecurity. Combatting the former may well make significant contributions toward the latter. Indeed, one-third of pirate sites link to malware,[56] pirate sites are 28 times more likely to infect their users with malware than similar mainstream websites, [57] and video streaming "has become the number one method to propagate highly dangerous malware on the Internet."[58] Hackers have

---

[54] 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 (May 2018), https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

[55] *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Exec. Order No. 13800, sec. 2(d) (May 11, 2017), 82 Fed. Reg. 22391, 22393 (May 16, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

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

[57] *Id.*

[58] Association of Internet Security Professionals, *Illegal Streaming and Cyber Security Risks* (2014).

already begun to exploit streaming piracy devices and add-ons to infect consumers.[59] When it comes to just one such recent exploit using closed captioning to spread malware over these devices, a security firm has estimated "there are approximately 200 million video players and streamers that currently run the vulnerable software, making this one of the most widespread, easily accessed and zero-resistance vulnerabilities reported in recent years," adding that streaming media players used to access pirate cites are also vulnerable to the hacking.[60] In another instance, a different security firm observed that certain software on these devices is vulnerable to "man in the middle" attacks.[61]

D. What the Private Sector is Doing to Address the Problem

Combatting the growth of streaming piracy requires coordination among all parties in a position to make a difference, including:

- cooperation among on-line marketplaces, payment processors, advertisers, domain name providers, website and file hosting providers, and search and social media services to choke off the distribution of, and funding to, pirate sites and services;
- civil and criminal actions against creators of pirate add-on software and the repository web sites that host them, against distributors of the preloaded devices, and against the entities streaming the content.

Toward that end, the MPAA and a broad array of stakeholders harmed by the spread of preloaded streaming piracy devices have formed a loose coalition aimed at educating policymakers and the public about the threats of streaming piracy devices and applications. In addition, the

---

[59] Digital Citizens Alliance, Alert, *Close Captioned for the Security Impaired: How the leaky system of illicit streaming devices poses a malware threat to consumers* (July 2017), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA-%20Closed%20Captions-Final.pdf.

[60] *Id.* (quoting security firm Check Point).

[61] *Id.*

Motion Picture Association's six studios, Netflix and Amazon Studios have come together to establish the Alliance for Creativity and Entertainment, "a global coalition of leading content creators and on-demand entertainment services committed to supporting the legal marketplace for video content and addressing the challenge of online piracy."[62] Beyond the eight founding members, ACE comprises more than twenty additional global media brands affected by streaming piracy.[63] To date, ACE has initiated three civil suits on behalf of its global membership to address the growth of illegal piracy devices and applications. One of those suits has already resulted in a preliminary injunction against a device seller[64] and an order for the seller to stop facilitating access to piracy.[65]

The MPAA and its members are also engaged in a number of voluntary initiatives to curb streaming-device-based piracy and other online IP theft, including collaborations with:

- Amazon and eBay on measures to keep piracy devices and applications off their online marketplaces.
- The Trustworthy Accountability Group, a private-sector effort between the advertising and content communities, to keep household brand advertising off of piracy sites.[66]
- Payment processors such as Mastercard, Visa, and Paypal to prevent pirates from using those organizations' financial networks to collect revenue from their unlawful online activities.

---

[62] *See* Alliance for Creativity and Entertainment, http://alliance4creativity.com.

[63] *See id.*

[64] *See id.*, *Court Grants Preliminary Injunction Against TickBox* (Jan. 30, 2018), https://alliance4creativity.com/news/court-grants-preliminary-injunction-tickbox/.

[65] *See id.*, *Court Orders Piracy Device Seller TickBox to Stop Facilitating Access to Unauthorized Movies and Television Shows* (Feb. 14, 2018), https://alliance4creativity.com/news/court-orders-piracy-device-seller-tickbox-stop-facilitating-access-unauthorized-movies-television-shows/.

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

These are all positive developments, but much work remains to be done. Other online platforms and internet intermediaries would do well to better emulate these types of voluntary initiatives. Unfortunately, many continue to fall short.

E. The Need for Federal Government Action

Another critical component in the battle against illicit streaming devices and applications is criminal action by the federal government. While the civil suits brought by the private sector are impactful, criminal actions by the federal government have a larger deterrent value, and thus would be even more effective at mitigating the problem. Although not a streaming device case, the federal government's criminal action against Megaupload, then the largest piracy "cyberlocker," accounting for 4 percent of all Internet traffic, prompted many other pirate operations to shutter, and resulted in an 6.5 to 8.5 percent increase in digital sales for three major studios in 12 countries.[67] We would expect similar results were the government to become more active in the fight against streaming devices.

To that end, the MPAA has 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 actions. Vishal Amin, the Intellectual Property Rights Enforcement Coordinator housed in the White House, has also convened stakeholders and federal

---

[67] BRETT DANAHER AND MICHAEL D. SMITH, GONE IN 60 SECONDS: THE IMPACT OF THE MEGAUPLOAD SHUTDOWN ON MOVIE SALES 4 (Sept. 2013), https://poseidon01.ssrn.com/delivery.php?ID=301002120071065118066119067099111105032027023067011038006025014072079079068030111101021018111115103010043004024094109124099089098074087007053118110115000101009087005014023020076122018088079086079007000107003031029030076028010107092082006006083119069&EXT=pdf.

agencies to discuss the issue. One result of that 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, which they graciously agreed to do.[68]

We would welcome the NTIA's voice in urging its sister agencies to bring criminal actions, as well as its consulting with the Customs and Border Patrol about the possibility of interdiction of illicit streaming devices entering the country from abroad. The NTIA might also query whether the FTC can bring enforcement actions against those marketing or distributing the devices, perhaps for fraud in their representations about the legality of the devices, or for harm to consumers stemming from malware. NTIA efforts to help raise the profile of this issue with foreign governments, as well as to share information with them and coordinate countermeasures, would also be beneficial. Educating consumers and policymakers about the harms of these devices, including the threat to the market for American digital products and services, could also pay dividends.

Conclusion

The internet ecosystem has changed dramatically over the last two decades—in most ways for the better. But the technology advances that have improved lives, created new business opportunities, and served as a catalyst for innovation can also be abused, and serve as a foundation for illicit and harmful behavior.

As the NTIA considers how best to encourage growth and innovation for the internet and internet-enabled economy, it is necessary to ask whether the internet polices our nation adopted twenty years ago to help nascent online platforms grow, are now subverting the NTIA's goals of

---

[68] 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.

protecting and promoting an open and interoperable internet, advancing the free flow of information, supporting the multistakeholder approach to internet governance, buttressing both privacy and security, and strengthening the global marketplace for American digital products and services. In particular, the NTIA should examine: 1) whether the law's broad liability limitations in favor of online platforms is exacerbating a variety of internet ills; 2) whether ICANN's lack of focus on accountability is jeopardizing faith in the multistakeholder model, and whether an overbroad application of the GDPR is threatening the safety, security, and stability of the internet; and 3) whether the rise of streaming piracy devices poses a threat to consumers, cybersecurity, and the market for American digital products and services. The NTIA should also advocate for the inclusion of strong copyright provisions in trade agreement and counsel its interagency colleagues not to export limitations on liability for online platforms.

Content creators and online platforms must, and often do, work together. We need each other. Content without distribution is the proverbial tree in the forest. And distribution without creative, compelling content is akin to watching paint dry—or endless cat videos.

Over the past twenty years or so, the content industry has been asked to take a hard look at itself and consider whether it was time to make adjustments to its business models in light of changes in the media landscape. The industry did just that, and there are now more than 140 lawful online services in the U.S. providing access to movies and television programming, and audiences used those services to access 110 billion television episodes and 8 billion movies in 2016 alone.[69] Also in 2016, there were 454 original scripted series, twice as many as in 2009.[70] To protect that

---

[69] *See* MPAA, https://www.mpaa.org/what-we-do/fostering-innovation/. Underlying data on internet transactions provide by IHS Markit. *See* www.IHS.com.

[70] FX Networks Research (2017).

growth, the MPAA member studios have entered into a variety of voluntary initiatives with advertisers, payment processors, and online marketplaces to make sure that the services of responsible actors do not facilitate the illicit and abusive actions of others.

The time may now have come for online platforms to take a hard look at their own practices and business models—and for government to take a hard look at past policy choices—in light of changes in the internet the landscape. Those choices may have made sense when the internet was nascent. But the internet is nascent no longer, and the grand experiment is starting to fail. By acting responsibly and collaboratively to keep digital neighborhoods safe for communication, commerce, and creativity, online platforms and internet intermediaries could help ensure we realize the vision we all have for the internet. Our hope is that more online platforms will work with us and others to promote the best of the internet and keep it safe, secure, and sustainable.