

National Telecommunications and Information Administration
Stakeholder Engagement on Cybersecurity in the Digital Ecosystem
Docket No. 150312253-5253-01

Comments of the Motion Picture Association of America

May 27, 2015

I. Introduction

The Internet is a tremendous tool for creativity, commerce and communication. Unfortunately, criminal enterprises are also using the Internet to hack into networks and computers for the purpose of stealing valuable data—whether personally identifiable information, trade secrets, or content. They are also using Internet ads, as well as pirated content and software or other “bait,” to fund their efforts and lure Internet users into revealing sensitive information, inadvertently download malware, or unknowingly becoming a node in a botnet. One-third of the 589 largest ad-supported content theft sites examined in 2014, for example, not only generated millions of dollars in revenue, but also included malware that could infect users’ computers, according to a recent study commissioned by the Digital Citizens Alliance.¹

In this proceeding, the Department of Commerce’s Internet Policy Task Force “is requesting comment to identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers.”² As the voice of the motion picture, home video, and television industries, the MPAA submits this filing on behalf of its members: Paramount Pictures Corp., Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corp., Universal City Studios LLC, Walt Disney Studios Motion

¹ DIGITAL CITIZENS ALLIANCE, GOOD MONEY STILL GOING BAD: DIGITAL THIEVES AND THE HIJACKING OF THE ONLINE AD BUSINESS 2, 9 (2015).

² Request for Comment, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 Fed. Reg. 14360, 14360 (NTIA Mar. 19, 2015).

Pictures, and Warner Bros. Entertainment Inc. We and they are committed to promoting a safe, secure, and stable Internet that everyone can enjoy.

Below we briefly describe a number of issues that would benefit if parties came together to explore coordinated, voluntary action through principles, practices, and guidelines.³ Some positive steps are already underway, which we indicate below,⁴ but more could be done. In some cases, the discussions may result in contractual or informal commitments to collaborate in particular ways, to engage in certain activities, or to refrain from particular conduct; in others, they may yield generally accepted standards of behavior for parties to abide to gain the blessing of an accreditation organization or some other seal of approval.⁵

Much of the Internet's success is attributable to its decentralized nature. Because no one entity controls it, anyone around the globe can contribute to the Internet's content and architecture. But that also means no single entity can solve problems when they arise. Consequently, no one set of players can or should be responsible for curbing harmful conduct on the Internet. Doing so will require cooperation among all stakeholders,⁶ a sentiment both we and the Internet Association echoed in recent correspondence to the House Judiciary Committee.⁷ The support for that sentiment from groups such as the Internet Association gives us hope that parties across the ecosystem—including government, content creators, search engines,

³ See *id.* at 14361 (asking in question 1 what security challenges could be addressed through voluntary action).

⁴ See *id.* (asking in question 1(v) for commenters to indicate “[w]hat pre-existing organizations and work already exist on the topic”).

⁵ See *id.* (asking in question 1(iv) “[w]hat form an actionable outcome might take”).

⁶ See *id.* (asking in question 1(i) for commenters to indicate why the topics they raise are “a good fit for a multistakeholder process”).

⁷ See Letter from Christopher H. Dodd, Chairman and CEO, MPAA, to House Judiciary Committee Chairman Bob Goodlatte and Ranking Member John Conyers, Jr., at 2 (April 29, 2015); Letter from Michael Beckerman, President and CEO, Internet Association, to House Judiciary Committee Chairman Bob Goodlatte and Ranking Member John Conyers, Jr., at 3 (April 29, 2015).

advertising networks, payment processors, and domain name registries and registrars—can come together to hold accountable those who would use the Internet for ill, and to stem or at least not abet the misdeeds of others.⁸

The Internet Policy Task Force “proposes to facilitate one or more multistakeholder processes around key cybersecurity issues facing the digital ecosystem and economy.”⁹ The IPTF notes that “[m]ultistakeholder processes, built on the principles of openness, transparency, and consensus, can generate collective guidance and foundations for coordinated voluntary action[,] ... includ[ing] voluntary policy guidelines, procedures, or best practices.”¹⁰ We agree.

II. *Specific Stakeholder Initiatives*

Even absent government involvement, a good deal of collaboration is already taking place to prevent both the theft of personally identifiable information, trade secrets, and content, as well as the use of content as bait for additional nefarious purposes. We welcome, nonetheless, efforts by legislative, executive, and regulatory officials to further encourage these kinds of voluntary initiatives. If pursued consistently, comprehensively, and collaboratively, we believe efforts in the following areas can help enhance cybersecurity by minimizing the harms from cyber-theft as well as reducing the likelihood of theft and breaches in the first place. Because the threats and the technological mechanisms parties use to perpetrate them evolve continuously, we do not believe the voluntary initiatives meant to address them should have a finite beginning or end. They will, by nature, be iterative, with few solutions likely to be perfect from the outset.¹¹

⁸ See Request for Comment, 80 Fed. Reg. at 14361 (asking in question 1(i) for commenters to indicate “whether stakeholders might reasonably be expected to come to some consensus”).

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.* (asking in question 1(iii) for commenters to indicate how long an initiative on each topic should take).

Because each initiative can itself involve multiple parties in multiple fora in an overlapping fashion, and does not necessarily need any particular official to commence, control, or terminate the discussion, we do not see that as a problem. Government actors can, of course, potentially endorse or participate in various initiatives at various stages.

Content creators can and should make content securely available online, as well as provide tools so audiences can find lawful sites and avoid those that not only provide content in an infringing manner, but may also engage in additional unlawful behavior in the process. Today, more than 400 services globally are making film and television content available lawfully online, with more than 100 of those services here in the United States. Consumers used those U.S. services to access more the 5.7 billion movies and 57 billion television episodes in 2013 alone. For our part, the MPAA has created WhereToWatch.com, a site that allows consumers to search for films and television programming by title, director, or actor, and enables them to click through to legitimate sources for accessing them.

Additional efforts by all players in the ecosystem to steer audiences toward lawful providers of content¹² and away from those engaged in illicit activity can prevent theft of sensitive information as well as the spread of malware¹³ that facilitates the formation of botnets¹⁴ and other tools for cyberattacks. Government can also play a role in this regard. For example, information campaigns advising consumers on best practices for avoiding cyber threats can refer consumers to resources such as WhereToWatch, thereby helping guide them in the direction of legitimate services and away from sites where they might compromise personal information or their own cybersecurity.

¹² See *id.* at 14362 (asking in question 2(h) about trusted downloads).

¹³ See *id.* (asking in question 2(e) about malware).

¹⁴ See *id.* (asking in question 2(a) about botnets).

Internet service providers can and should educate their users about potential harms and unlawful activity on the Internet. In that vein, we appreciate the participation of those ISPs involved in the Copyright Alert System, which we believe is positive. We also note, as discussed above, that all voluntary initiatives are iterative, and few will be perfect straight out of the box. Additional discussion and effort around notice programs and other ISP efforts can help strengthen this link in the online chain.

Search engines, as the gateway to the Internet, can and should promote legitimate sites in their search results, as well as demote, de-index, or at the very least warn consumers of those sites that consistently engage in unlawful behavior. This is an area that requires persistent and collaborative effort by all participants. We note, for example, that Google has sought to alter its algorithm to demote pirate sites, an effort that we appreciate. We also note, however, that other pirate sites or sometimes even variants of the same site float right back to the top. Further work in this and similar areas should be encouraged.

Advertisers and advertising networks can and should prevent legitimate ads from appearing on—and thus funding—sites engaged in illicit activity, as well as prevent ads from spreading malware that facilitates cybercrime.¹⁵ To that end, we find encouraging the Trustworthy Accountability Group’s creation of the Brand Integrity Program Against Piracy.¹⁶ The TAG was created by the Association of National Advertisers, the American Association of Advertising Agencies, and the Interactive Advertising Bureau to fight ad-supported piracy and malware, among other things. The TAG’s BIPAP program is intended to help advertisers and ad

¹⁵ See *id.* (asking in question 2(g) about “malvertising”).

¹⁶ See Advertising Industry Launches Initiative to Protect Brands Against Piracy Websites: Trustworthy Accountability Group Launches Anti-Piracy Program as First Part of Campaign Against Fraud, Malware, Lack of Transparency (Feb. 10, 2015), available at https://www.iab.net/media/file/TAG_Anti-Piracy_Release_final_IAB.pdf.

agencies prevent placement of ads on websites associated with unlawful activities, such as content piracy and dissemination of counterfeit goods. Under the BIPAP program, the TAG will work with independent third parties to certify advertising technology companies as Digital Advertising Assurance Providers. The DAAPs will identify risky websites and help companies avoid them. Encouraging initiatives such as these could help reduce profits for and minimize consumer exposure to websites that create or exploit weaknesses in cybersecurity.

Payment processors also can and should prevent their services from facilitating the flow of money to websites engaged in illicit activity. While Internet advertising is one source of funding for sites engaged in cyber-related activity, subscription revenue or one-time payments are another. Such payments are often made through services offered by payment processing companies such as PayPal, MasterCard, and Visa. Those companies have started adopting policies and practices to prevent websites engaged in illegal activity, such as illicit cyberlockers, from benefiting from their payment networks. We commend such efforts and encourage further conversation around these types of voluntary initiatives.

Domain name registries, registrars, and ICANN can and should enforce their existing contractual provisions that prohibit the use of domain names for illegal conduct and require investigation of complaints.¹⁷ Since at least 2001, ICANN has prohibited every registrant of a generic top-level domain name from “directly or indirectly” infringing the rights of others. The ICANN Public Interest Commitments obligate all new gTLD registries to require registrars to prohibit registrants from distributing malware, stealing intellectual property, committing fraud, or engaging in other illegal activity, as well as to enforce those requirements. ICANN’s 2013 Registrar Accreditation Agreement requires registrars to take reasonable and prompt steps to

¹⁷ See Request for Comment, 80 Fed. Reg. at 14362 (asking in question 2(b)-(c) about naming infrastructure and the Domain Name System).

investigate reports of abuse, and to take commercially reasonable steps to ensure domain names are not used to infringe the rights of thirds parties.

These obligations were intensively negotiated for years, opened to the entire multi-stakeholder community for public comment, and approved by the ICANN board. Yet ICANN does not appear to be enforcing these provisions, as discussed at the May 13, 2015, House Judiciary Committee hearing regarding “Stakeholder Perspectives on ICANN.”¹⁸ Enforcing these provisions would go a long way toward shutting down illegal sites, many of which may be facilitating cybercrimes. Enforcing these provisions would also go a long way toward providing the transparency, creditability, and accountability necessary for the multistakeholder model of Internet governance to succeed, and to instill the kind of confidence the public and private sector need for the online ecosystem to thrive.

III. Conclusion

As the IPTF points out, “there are real, evolving threats in cyberspace that not only put businesses and their online operations at risk, but threaten to undermine the trust on which much of the digital economy depends.”¹⁹ Illegal activity online—including theft of personal information and intellectual property—not only presents such risk to business operations and trust in the ecosystem,²⁰ but also serves as sources of funding and a mechanism for spreading malware that perpetuates further threats to cybersecurity. The parties engaged in such theft are often either exploiting or creating cybersecurity threats, such that efforts to stop them will likely enhance cybersecurity.

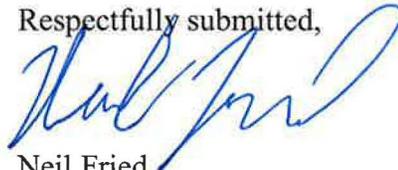
¹⁸ See <http://judiciary.house.gov/index.cfm/2015/5/hearing-stakeholder-perspectives-icann>.

¹⁹ Request for Comment, 80 Fed. Reg. at 14360 (citing U.S. Department of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy* (June 2011)).

²⁰ See *id.* at 14362 (asking in question 2(f) about web security and trust).

For that reason, we believe promoting and pursuing the types of voluntary initiatives above will benefit both multistakeholderism generally and cybersecurity in particular, to the ultimate benefit of all stakeholders in the digital ecosystem.²¹ To again quote the Federal Register notice, these are “discrete security challenges in the digital ecosystem where collaborative voluntary action between diverse actors can substantially improve security for everyone.”²² And while we do not necessarily need the IPTF to coordinate the actual voluntary initiatives themselves, added government attention to, and support for, their importance can certainly advance their development. We therefore would welcome efforts by the IPTF to “facilitate a series of discussions around [these] cybersecurity challenges that may be addressed through a better shared understanding of the nature of the problem, [since] multistakeholder discussion can be a catalyst for self-coordination.”²³

Respectfully submitted,



Neil Fried
SVP, Government and Regulatory Affairs
Motion Picture Association of America
1600 I Street NW
Washington, D.C. 20006
(202) 293-1966

²¹ See *id.* at 14361 (asking in question 1(ii) for commenters to explain “[w]hy such a process would benefit the digital ecosystem as a whole”).

²² *Id.*

²³ *Id.* (citing U.S. Department of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy* (June 2011)).