Independent Film & Television Alliance®

10850 Wilshire Boulevard / 9th Floor
Los Angeles, CA 90024-4321
310-446-1000 TEL / 310-446-1600 FAX
www.ifta-online.org / info@ifta-online.org

May 18, 2015

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW., Room 4725
Attn: Cybersecurity RFC 2015
Washington, DC 20230

Via Electronic Mail to securityRFC2015@ntia.doc.gov

Re: Request for Public Comment on Stakeholder Engagement on Cybersecurity in the Digital Ecosystem issued by the National Telecommunications and Information Administration, U.S. Department of Commerce. Docket No. 150312253-5253-01[1]

The Independent Film & Television Alliance[2] (IFTA) respectfully submits these comments in response to the Notice of Inquiry referenced above.

I. Cybersecurity and Copyright Protection

Copyright infringement is a major form of cybercrime which is of significant importance to the independent film and television industry. The production, financing and distribution models of the independents differ substantially from those of the U.S. major studios in that independent producers secure financing and distribution for each project on a territory-by-territory basis through licensing deals with local (national) distributors.[3] National distributors seeking to license independent films assess the value of the project (gross receipts across all distribution media)[4] and may enter into license agreements with the producer that provide minimum guarantees (minimum license fees to be paid) to secure the exclusive distribution rights to the project in advance of production. Those license agreements are used by the

[1] Request for Public Comment on Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 Fed. Reg. 14360 (Mar. 19, 2015). (http://www.gpo.gov/fdsys/pkg/FR-2015-03-19/pdf/2015-06344.pdf)

[2] Based in Los Angeles, California, IFTA is the global trade association of the independent film and television industry. Our nonprofit organization represents more than 140 Member Companies in 21 countries consisting of the world's foremost independent production and distribution companies, the majority of which are small to medium-sized U.S.-based businesses (a complete list of IFTA Member companies is available online at http://www.ifta-online.org). Independent films and television programs, those financed in majority part without reliance on the six U.S. "major studios" and for which the production company controls distribution in a majority of territories worldwide, are made at every budget level and may be mainstream, commercial or art house. The independent sector produces approximately 75% of all U.S. films annually and globally produces more than 400 films and countless hours of television programming each year resulting in more than $4 billion in annual worldwide revenues. IFTA regularly provides input to governments around the world on a wide range of copyright, trademark, financing and export issues that impact our industry.

[3] The U.S. major studios self-finance and distribute their productions through their own worldwide distribution subsidiaries.

[4] Factors used in assessing the value of a project include the script, director, writer or key cast; subject matter or genre; estimated production budget; and projected season and year of release.

producer as collateral for production loans to fund the production. Such financing deals depend largely on the confidence of local distributors and financiers that they will recoup on their investment from the exploitation of the completed film; which is significantly diminished when a film is the subject of rampant online piracy. Therefore, without proper copyright protection, independent producers would not be able to obtain the production financing required to create their content.

Expanded opportunity for online distribution of film and television programming has expanded the scope of online theft and diminished the ability of any producer to protect his work long enough to even repay third-party investments. Thus, the need for effective cybersecurity measures to protect rights holders and consumers is urgent. Copyright protection must be included in any cybersecurity discussion because: 1) cyber-attacks are a major source of unauthorized audiovisual content; 2) users who access unauthorized content are subject to malware and other threats; and 3) basic indicators of authenticity attached to sites that feature only illegally obtained content builds trust among unwitting users.

a. Source of Unauthorized Content

Cybersecurity plays a major role in how illegal copies of digital content are obtained.[5] Recent technological improvements have provided additional opportunities for audiovisual content owners to reach their consumers through various digital distribution platforms.[6] However, by making high-quality digital files available, companies are opening themselves up to the significant risks that such files will be obtained through unauthorized means and then redistributed broadly over the Internet to millions of would-be paying consumers.[7] It is important to engage all stakeholders in the discussion of cybersecurity, including smaller copyright owners who have not had the benefit of established security standards to address these risks.

b. Threats to Consumers

In addition to the significant harm to the creative industries, particularly independent producers, online copyright infringement poses substantial dangers to consumers who, either knowingly or unknowingly, access this unauthorized content. Reports have shown that 97% of illegal streaming websites contain malware.[8] Unlike traditional scamming methods in which a user has to make a conscious decision to open a suspicious email or link, malware through illegal streaming is activated in the background while the user is immersed in the viewing experience, and the hacker is able to obtain access through the P2P protocol.[9] These illegal streaming websites do not provide the security protocols offered by legitimate online distributors leaving unknowing users vulnerable to attack.[10]

---

[5] *See* Andrew Wallstein, "Sony's New Movies Leak Online Following Hack Attack", *Variety*, November 29, 2014, available at http://variety.com/2014/digital/news/new-sony-films-pirated-in-wake-of-hack-attack-1201367036/.
[6] *See* "Broadcom Launches Enhanced 5G WiFi Video Streaming for the Home", January 6, 2014, available at http://www.broadcom.com/press/release.php?id=s817141.
[7] *See* Todd Spangler, "Top 20 Most Pirated Movies of 2014 Led by *Wolf of Wall Street*, *Frozen*, *Gravity*", *Variety*, December 28, 2014, available at http://variety.com/2014/digital/news/top-20-most-pirated-movies-of-2014-led-by-wolf-of-wall-street-frozen-gravity-1201388403/.
[8] *See* AISP Working Paper, "Illegal Streaming and Cyber Security Risks: A Dangerous Status Quo?", Autumn 2014, available at http://cryptome.org/2014/09/illegal-streaming-malware-epoch-times-full-14-0923.pdf.
[9] *Id.*
[10] *Id.*

c. Indicia of Authenticity

Some pirate sites offer sophisticated user interfaces that give an air of legitimacy, which may lead a misinformed user to believe that the site and content offerings are "legitimate" when in fact the user is being exposed to cybersecurity threats by viewing unauthorized films and television programming.[11] Furthermore, pirate websites will often use legitimate payment processors (and their logos) or feature advertisements in order to create the perception of authenticity and generate revenue.[12] In response, U.S. industry has recently adopted the payment system operators' "Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet"[13] and the "Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting."[14] Both are intended to reduce online infringement by making counterfeiting and infringement a less profitable business by cutting off revenue to sites that are "principally dedicated to selling counterfeit goods or engaging in copyright piracy and have no substantial non-infringing uses"[15] and eliminating the indicia of credibility that attaches to rogue sites from legitimate advertisements, credit card logos and payment processing.

II. Voluntary Initiatives in Cybersecurity

IFTA supports the use of private voluntary agreements as one tool to reduce cybercrimes, including copyright infringement, and make consumers aware of the availability of legitimate content. However, voluntary agreements can easily fall short of offering full protection to consumers or to individual rights holders who urgently need to address the theft and proliferation online of a single title. Even in the best circumstances, voluntary agreements may fail to meet their objectives through simple failure by service providers to act in line with "Best Practices." Government must fill the gaps by leading the effort to ensure that any voluntary initiatives are robust and effective.

Given the technological complexities of all cybercrimes, including copyright infringement, as well as the social and financial implications, it is imperative to ensure that any such process has the direct involvement of all stakeholders – including content owners, technology companies, ISPs, advertisers and ad placement agencies, payment processors, consumer groups, governments, and international governmental originations – in crafting effective means to recognize and prevent online infringement. The government must act as convener of such groups and exercise oversight to ensure that all stakeholders are actively included and involved in "industry at large" discussions and solutions.

---

[11] *See* Jeff Stone, "Is Popcorn Time Safe? Pirate Bay, Netflix Comparisons Provide Little Legal Clarification", *International Business Times*, September 20, 2014, available at http://www.ibtimes.com/popcorn-time-safe-pirate-bay-netflix-comparisons-provide-little-legal-clarification-1692417.

[12] *See* "Online Pirates Thrive on Legitimate Ad Dollars", *Los Angeles Times*, June 3, 2014, available at http://www.latimes.com/business/la-fi-0604-piracy-ddvertising-20140603-story.html#page=1.

[13] *See* 2012 U.S. Intellectual Property Enforcement Coordinator Joint Strategic Plan, available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_two-year_anniversary_report.pdf.

[14] *See* "Coming Together to Combat Online Piracy" posted by *Victoria Espinel, U.S. Intellectual Property Enforcement Coordinator,* available at http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting.

[15] Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting (developed by 24/7 Media, Adtegrity, AOL, Condé Nast, Google, Microsoft, SpotXchange, and Yahoo!)

Finally, while best practices and voluntary agreements are useful for rights holders and may protect consumers, a strong legal framework to address cybersecurity and copyright infringement in the online environment is necessary to ensure that all stakeholders and consumers are protected from the critical consequences of security breaches and cybercrime that are the trigger points for copyright infringement.

III. Conclusion

IFTA thanks the National Telecommunications and Information Administration for commencing this Request for Public Comment and other related RFCs to gather comments from all stakeholders on such important issues. Public consultations such as this will provide invaluable information and establish strong foundations for the government and stakeholders to move forward with economic development on the Internet by addressing cybersecurity and online infringement comprehensively, including providing appropriate legislation or frameworks and solutions to protect copyright, and encouraging private and transparent voluntary mechanisms which encompass the interests and the needs of all stakeholders and the public. Although other NTIA processes have focused on improving the efficiency of existing copyright protection measures between content owners and the ISPs, it is important to recognize online copyright infringement as a cybercrime and examine these topics, including the implications of the crimes involved, within the realm of cybersecurity.

Respectfully Submitted,

Independent Film & Television Alliance

/s/
Jean M. Prewitt, President & CEO
10850 Wilshire Blvd., 9th Floor
Los Angeles, CA 90024-4321