October 25, 2021

Trisha B. Anderson
Deputy Assistant Secretary, Intelligence & Security
U.S. Department of Commerce

Re: Advance Notice of Proposed Rulemaking
Executive Order 13984 of January 19, 2021
Taking Additional Steps to Address the National Emergency
With Respect to Significant Malicious Cyber-Enabled Activities
Docket number: DOC-2021-0007

Dear Ms. Anderson,

The Motion Picture Association, Inc. ("MPA") is pleased to submit these comments to the Department of Commerce ("the department") in response to the Advance Notice of Proposed Rulemaking ("ANPRM") issued on September 24, 2021.

I. Introduction

The MPA serves as the global voice and advocate of the motion picture, television, and streaming industry. It works in every corner of the globe to advance the creative industry, protect its members' content across all screens, defend the creative and artistic freedoms of storytellers, and support innovative distribution models that bring an expansion of viewing choices to audiences around the world. Its member studios are: Walt Disney Studios Motion Pictures; Netflix, Inc.; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; and Warner Bros. Entertainment Inc.

The American motion picture and television industry is a major U.S. employer that supported 2.5 million jobs and $188 billion in total wages in 2019. This includes 331,000 jobs in the core business of producing, marketing, and manufacturing motion pictures, television shows and video content, as well as 579,000 jobs in the distribution of motion pictures, television shows, and video content to consumers, including people employed at movie theaters, television broadcasters, cable companies, and online video services. The industry also supports indirect jobs in the thousands of companies that do business with the industry, such as caterers, dry cleaners, florists, hardware and lumber suppliers, and

retailers. This is a nationwide network of mostly small businesses representing every state in the country, with 87 percent employing fewer than 10 people.[1]

We agree with the premise of E.O. 13984: there is a clear need to act to curb the damage inflicted by "*malicious cyber actors [who] aim to harm the United States economy through the theft of intellectual property*",[2] such as copyrighted works. Online content theft continues to pose the most significant and evolving threat to our industry. In 2018, there were an estimated 190 billion global visits to piracy sites.[3] This piracy costs the U.S. economy at least $29.2 billion in lost revenue each year.[4] This large-scale for-profit commercial piracy undercuts legitimate streaming services and ultimately hurts American consumers and businesses.

Online copyright infringement also creates significant cyber security risk: purveyors of copyright-infringing content often lace the sites and devices through which they operate, and the files they distribute, with malware. In 2015, an investigation by the Digital Citizens Alliance (DCA) and RiskIQ found that a third of a sample of 800 sites dedicated to distributing infringing copies of movies and television shows exposed their users to malware, 45% of which was automatically downloaded and installed on the user's machine without requiring the user to click anything.[5] Another DCA investigation found malware on apps preloaded onto illicit streaming devices[6] that stole user names and passwords, probed the user's network and surreptitiously uploaded data from the user's device.[7] Further research from Carnegie Mellon University has established a clear correlation between the time spent on copyright-infringing sites and the likelihood of downloading malware.[8] In short, the link between online copyright infringement and cybercrime is clear, which is why the 66 parties – including the United States – to the Council of Europe Convention on Cybercrime decided to include online copyright infringement among the cybercrimes that are proscribed under the Convention.[9]

MPA works around the world to investigate, disrupt and terminate the operations of, and bring legal cases against, the perpetrators of commercial scale online copyright infringement. In many of these efforts, we collaborate closely with civil, administrative and criminal law enforcement agencies in the U.S. and internationally, including the U.S. Departments of Justice and Homeland Security and Interpol.

---

[1] The American Motion Picture and Television Industry – Creating Jobs, Trading Around the World. The Motion Picture Association, April 8, 2021, https://www.motionpictures.org/wp-content/uploads/2021/06/MPA_Economic_contribution_US_infographic_2019_032521.pdf

[2] See the E.O.'s preamble.

[3] MUSO, https://www.muso.com/magazine/global-piracy-hits-190-billion-visits-in-2018-but-uk-sees-a-drop

[4] Impacts of Digital Video Piracy on the U.S. economy. Blackburn, Eisenach, Harrison Jr., June 2019. https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf

[5] Digital Bait : How Content Theft Sites And Malware Are Exploited By Cybercriminals To Hack Into Internet Users' Computers And Personal Data, Digital Citizens Alliance and RiskIQ, December 2015, https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf

[6] These devices are functionally similar to the USB and HDMI dongles that can be connected into a TV to access legitimate streaming services, but are preloaded with apps that connect to illegal streaming sites.

[7] Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm, Digital Citizens Alliance, April 2019, https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

[8] Does Online Piracy Make Computers Insecure? Evidence from Panel Data, Rahul Telang, Carnegie Mellon University, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3139240

[9] Convention on Cybercrime of the Council of Europe, Title 4 – Offences related to infringements of copyright and related rights.

However, these enforcement efforts are hindered when providers of Infrastructure-as-a-Service ("IaaS") fail to take adequate steps to ensure their services are not being used to facilitate malicious cyber activities – including copyright infringement – by bad actor customers who use their services for illicit commercial purposes. This problem is compounded by the fact that piracy services can be operated anonymously or pseudonymously. All stakeholders in the Internet ecosystem – including IaaS providers – should actively seek to reduce support for malicious cyber actors.

Section 512(h) of the Digital Millennium Copyright Act provides a tool for rightsholders to obtain from certain service providers "*information sufficient to identify*" alleged infringers by means of court-issued subpoenas, "*to the extent such information is available to the service provider.*" 17 USC 512(h)(3). To the extent such information is not available to the service provider, however, or if the provided information is false, this tool cannot be effective.

For these reasons, MPA lauds the Administration's recognition of the role of IaaS in intellectual property theft; the imperative of more robust record-keeping practices, user identification and verification standards; and the utility of best practices to deter abuse of U.S. IaaS products by their business customers and support accountability for victims of large-scale commercial piracy operations.

II. Comments in response to specific questions in the ANPRM

Question (1)a. How should the Department implement the requirement for both verifying a foreign person's identity (1) upon the opening of an Account, and (2) during the ''maintenance of an existing Account,'' and what should the Department consider in determining customer due diligence requirements for U.S. IaaS providers?

In our experience, malicious cyber actors – including operators of piracy sites and services – almost always misrepresent their identity to IaaS providers. The regulations should therefore ensure that the verification of their identities generates a high degree of confidence that the recorded identities are genuine.

We also support the E.O.'s requirement that business customer identities be verified not just upon the opening of an account but also during its maintenance. To implement this requirement, we believe that business customer information should be updated at appropriate times on a risk-sensitive basis.

Question (1)b. Can the Department implement the requirement to verify a foreign person's identity (1) upon the opening of an Account, and (2) during the ''maintenance of an existing Account,'' while minimizing the impact on U.S. persons' opening or using such Accounts, or will the application of the requirements to foreign persons in practice necessitate the application of that requirement across all customers?

As a practical matter, MPA believes that meaningful verification of identity will and should necessitate verification of all IaaS business customers. Simply allowing them to self-identify as U.S. or foreign persons lacks the rigor sought in the Executive Order. Further, using indicators of presumed foreignness

– such as paying in foreign currency, providing a foreign postal address or connecting from a foreign internet protocol (IP) address – to trigger an identity verification would be inadequate, as such indicators would be easy to falsify. As a result, we believe that the regulations implementing E.O. 13984 should require that the identity of all business customers of IaaS providers be verified, and that the Department should reserve to foreign customers the identity recordation requirement.

Beyond the implementation of E.O. 13984, however, we see no principled reason why identity and recordation requirements should not go further and apply to all business customers of IaaS providers. While a significant share of malicious cyber activity – including copyright infringement – is perpetrated by non-U.S. commercial actors, U.S. business customers represent a non-negligible share of perpetrators of malicious cyber-enabled activities. Indeed, the extension of these identity verification and recordation requirements to U.S. business customers would facilitate the task of advocating the adoption of such requirements by U.S. trading partners.

However, we appreciate that the International Emergency Economic Powers Act (IEEPA), which provides the underlying statutory authority of E.O. 13984, requires a foreign nexus; we encourage the administration to implement this E.O. without delay while it uses or seeks additional authority to complement its requirements.

Question (1)d. Do U.S. IaaS providers currently collect information on the true users of their respective IaaS products, to include reselling activities?

In our experience, some IaaS providers collect identity information on the true users of their respective IaaS products and some do not. There are companies, for instance, whose business is to acquire domain names for the sole purpose of reselling them,[10] which is not necessarily nefarious but does create opportunities for evading identity verification and recordation. Other companies, however, act as domain name intermediaries precisely for the purpose of procuring and owning domain names on behalf of others to provide them with anonymity.[11] Therefore, MPA recommends that the regulations fully cover not only direct sales but also all types of resale.

Additionally, identity verification and recordation should occur regardless of the nationality or location of the reseller, so that resale by U.S. or foreign business customers to end-users is covered.

Question (2) What data protection and security implications should the Department be aware of when considering the imposition on U.S. IaaS providers of requirements to maintain records regarding foreign person customers? For example, how might the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or other relevant data protection and security laws and regulations affect U.S. IaaS providers'

[10] "Domains of Danger: How Website Speculators and Registrars Trade Internet Safety for Profit", Digital Citizens Alliance, August 2020, https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA-DOMAINS-OF-DANGER.pdf

[11] For example Njalla (located on the web at njal.la) is prominent among pirate services because it provides them anonymity and in so doing, complicates law enforcement efforts.

ability to fulfill these recordkeeping requirements pursuant to E.O. 13984? Should the Department consider specific limitations on the amount of time that such records must be kept?

Every year, MPA member studios invest billions of dollars in their brands and in their trusted relationship with audiences in the United States and around the world. We know that earning and maintaining consumers' trust is critical to all companies' mission as businesses and good corporate citizens. Thus, we fully support efforts to ensure that personal information is handled responsibly and safely by businesses delivering desired products and services to those consumers.

In the context of this E.O, we appreciate and support the goal of ensuring that identity verification and recordation is done in a manner that respects privacy rights. A core principle underlying many privacy laws, including the GDPR, is data minimization. While the GDPR does not prohibit the collection and provision of personal data associated with the registration and maintenance of websites, an effective way to minimize the collection of personal data is to apply the identity verification and recordation requirements to customers, whether legal entities or natural persons, acting with a business purpose, rather than a personal or consumer purpose.[12]

Question (4) What should the Department consider when deciding how compliance with the requirements adopted under Section 1 should be monitored and enforced (i.e., should compliance and enforcement be strictly limited to instances following malicious cyber activities that are traced back to specific U.S. IaaS providers; should the Department implement a voluntary or required proactive suspicious/abnormal Account activity report mechanism to assist in ongoing due diligence; should the Department periodically conduct compliance audits)? How should the Department verify that Section 1 requirements are being met?

We propose three measures to help ensure that the regulations are effective and that they are diligently implemented and complied with by IaaS providers. First, the regulations should require IaaS providers to make available a tool for any interested party to notify an IaaS provider in case there are reasonable grounds to believe one of its business customers has provided information that is false, misleading, or otherwise invalid. Making this tool easy to access and easy to use will facilitate its use in particular by small and medium size enterprises wishing to notify IaaS providers.

Second, the regulations should provide that, upon having reasonable grounds for believing that one of their business customers has provided information that is false, misleading, or otherwise invalid (including by receipt of a notice or when they verify and update the information), IaaS providers shall terminate all services to the business customer in question, unless the business customer sufficiently

[12] Note that the E.O.'s sec. 5(e) definition of IaaS product refers to "consumer", which could potentially restrict identity verification and recordation to customers who purchase goods or services for personal use. However, most IaaS products are business rather than consumer products. In fact, the use of "consumer" is inconsistent with the E.O.'s requirement to verify the identity of any "person", which the E.O. defines (in sec. 5(g)) as "an individual or entity." The definition of IaaS product uses the word "consumer" because it was borrowed from a NIST definition (see footnote below) that uses that word to distinguish between providers and consumers – i.e. users – of computing resources.

corrects or supplements the information or disputes the notice within a reasonable timeframe. The regulations should provide that any such correction or dispute shall be shared with the notifying party.

Third, the regulations should provide dissuasive financial penalties for non-compliance.

Supplement to question 12 (definition of "IaaS Product")

One of the most important provisions of this E.O. is the definition of an IaaS product in Sec. 5(e):

> "*any product or service offered to a consumer, including complimentary or ''trial'' offerings, that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications.*"

The E.O.'s definition of IaaS product was derived from Special Publication 800-145 of the National Institute of Standards and Technology.[13] While it is widely recognized as a seminal definition of cloud computing and of its different service models, including IaaS, it was not written for a regulatory purpose but to "*characterize important aspects of cloud computing and (…) to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing.*"[14] Its intended audience does not include regulators but "*system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services.*"[15]

As a result, this definition lacks the clarity of language and certainty of scope that is necessary for a regulatory definition. It thus requires interpretation and clarification.

To this end, we note that a narrow reading of this definition would significantly hinder the ability of law enforcement and other interested parties to discover the identity of malicious cyber actors – including piracy service operators – who utilize the full range of IaaS products to conduct, shield and monetize their operations. As the E.O.'s preamble notes, malicious cyber actors "*use United States IaaS products for a variety of tasks.*" In the course of our antipiracy investigations, MPA regularly interacts with providers of all manners of IaaS products that are utilized by malicious and notorious commercial piracy services.

Therefore, to properly effectuate the E.O. we believe it is important to ensure that a broad range of IaaS products are covered by the requirement to verify and record business customer identities. MPA recommends that the regulations clearly apply to providers of the following types of IaaS products:

- **Web hosting** is infrastructure essential to operating a website. From an enforcement perspective, the hosting provider has the ability to take malicious and copyright-infringing websites offline.

[13] See p.3 of Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[14] SP 800-145, p.2, sec. 1.2.
[15] SP 800-145, p.2, sec. 1.3.

- **Reverse proxies** funnel connections to many different websites through shared servers that then redirect each connection to its correct destination. A reverse proxy thus serves a crucial role for a malicious website: it thwarts efforts to locate its true location – the internet protocol (IP) address – and hosting provider.
- **Content delivery networks ("CDNs")** efficiently deliver content (in particular bandwidth-dependent content, such as video) to a global userbase by placing servers all around the world that store local copies of that content. One of the by-products of using a CDN is that, like a reverse proxy, it hinders enforcement efforts by masking the IP address and sometimes the hosting provider of a website.
- **Domain Name System ("DNS")** servers "resolve" (i.e. translate) a web address into the corresponding IP address. DNS resolution is an essential networking function of the internet and infrastructure that is essential to operating a website.
- **Anti-distributed denial of service attack ("anti-DDoS")** services protect legitimate sites against DDoS attacks, but are also utilized by malicious cyber actors – including copyright infringers – because they use DNS redirection to reroute a site's incoming traffic through filters, and as a result mask the site's IP address and web host.
- **Online marketplaces** are platforms that allow businesses and consumers to offer, sell and purchase goods and services. Alongside billions of legitimate daily transactions, online marketplaces have become susceptible to misuse and sales of illegal devices and services connecting consumers to copyright-infringing content.
- **Domain name registration** is an essential function performed by entities called registrars, which have the right to create and sell domain names. Registrars operate under the authority and supervision of registries.
- **Privacy proxies** enable users of IaaS products to pseudonymize the identity and contact information they give to IaaS providers, and thus evade enforcement efforts that may target them.
- **Advertising networks** place ads on behalf of advertisers on websites that display advertising, thus supporting copyright-infringing sites by providing them with considerable advertising revenue – an estimated 1.34 billion USD, according to the Digital Citizens Alliance.[16]
- **Payment processors** manage transactions and payments on behalf of merchants, including those who commerce in copyright-infringing content. They include payment card networks, payment card acquirers and other payment processing and money-transfer services.
- **Cryptocurrency exchanges** are entities that enable the conversion of hard currency into cryptocurrency, and vice-versa. Cryptocurrencies have become a popular method among malicious cyber actors – including copyright infringers – for anonymously receiving payments and storing profits.

III. Conclusion

In the U.S. and around the world, the motion picture and television industry is a community of creators and innovators who work tirelessly at the art and craft of storytelling. Large-scale providers of copyright-infringing content threaten the very heart of our industry and in so doing, threaten the livelihoods of the

[16] Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market, Auguste 2021, https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf

people who give it life. They are an immediate threat to legitimate commerce, impairing legitimate services' viability, curbing U.S. competitiveness, and putting American consumers at risk. Efforts by the department and administration to require customers of internet infrastructure services to verify their identity will improve online trust and accountability and are thus an essential step in fostering creativity and innovation, not only in the film and television industry but throughout the creative economy.

MPA appreciates the opportunity to comment and is ready to provide further information or answer questions as requested.

Sincerely,

Franck Journoud
Vice President, Federal Affairs & Technology Policy