Computer & Communications
Industry Association
Tech Advocacy Since 1972

Via Electronic Submission

October 16, 2017

Elizabeth Kendall
Acting Assistant U.S. Trade Representative for Innovation and Intellectual Property
Office of the United States Trade Representative
600 17th Street NW
Washington, D.C. 20006

Re: *2017 Special 301 Out-of-Cycle Review of Notorious Markets*

Dear Ms. Kendall:

Pursuant to the request for comments issued by the Office of the United States Trade Representative (USTR) and published in the Federal Register at 82 Fed. Reg. 38,987 (Aug. 16, 2017), the Computer & Communications Industry Association (CCIA)[1] submits the following rebuttal comments for consideration as USTR prepares its 2017 Special 301 Out-of-Cycle Review of Notorious Markets (Docket No. USTR-2017-0015).

CCIA's reply comments caution that USTR should not conflate critical, general technologies with the actions of a small minority of users whose infringements have been identified by commenters.

(1) CDNs and Reverse Proxies

Several responses to the Notorious Markets review offer generalized criticisms of providers of content delivery networks (CDNs) and reverse proxies, including CCIA member Cloudflare.[2]

[1] The Computer & Communications Industry Association ("CCIA") represents large, medium-sized, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services—companies that collectively generate more than $540 billion in annual revenues. A complete list of CCIA members is available at https://www.ccianet.org/members.

[2] RIAA Comments, ID No. USTR-2017-0015-0013, at 4 (complaining that it is difficult to track notorious websites due to widespread use of reverse proxy services as "more and more pirate sites employ reverse proxy services, most commonly Cloudflare, to obfuscate their IP address"); MPAA Comments, ID No. USTR-2017-0015-0011, at 11 (critiquing hosting providers and CDNs, including Cloudflare: "An example of a CDN frequently exploited by notorious markets to avoid detection and enforcement is CloudFlare, a CDN that also provides reverse proxy functionality," adding that "[g]iven the central role of hosting providers in the online ecosystem, it is very concerning that many refuse to take action upon being notified that their hosting services are being used in clear violation of their own terms of service prohibiting intellectual property infringement and, with regard to notorious markets such as those cited in this filing, in blatant violation of the law."); ESA Comments, ID No. USTR-2017-0015-0012, at 2 (claiming that "[a]pproximately half of the websites referenced in this document have a business relationship with a single U.S.-based CDN. Therefore, it is important that all U.S.-based CDNs join ISPs, search engines, payment processors, and advertising services that have successfully collaborated with rights holders in

These comments mischaracterize these types of services, which are critical to the safe, secure, and efficient operation of the Internet. These and other types of Internet 'middle-layer' infrastructure are widely utilized by the private and public sectors, and assist in the fight against everything from foreign denial-of-service attacks to malware spread by criminal hackers. Reverse proxy services essentially operate as a gatekeeper for other websites to intermediate the requests they receive from the wider Internet. Similarly, CDNs are geographically distributed networks of proxy servers that deliver content from an originating website to users worldwide, with their relative proximity to end-users providing improved availability and performance.

In these roles, reverse proxies and CDNs can provide a variety of functions. These include mitigating or rerouting malicious or voluminous requests like denial-of-service attacks or known malware, encrypting browsing activity, and reducing the load of serving content by caching or compressing data. Rather than being a nefarious technology, these services are instrumental to a multi-layered defense-in-depth security strategy. Websites belonging to journalists, media organizations, dissident political groups, and nonprofits regularly take advantage of reverse proxies and CDNs to reach audiences while protecting their identities and sensitive information from criminals and oppressive regimes.[3]

The U.S. Government itself advises the use of these technologies for cybersecurity purposes. For example, the National Institute of Standards and Technology (NIST) Guidelines on Securing Public Web Servers recommend reverse proxies,[4] as do NIST's Guidelines on Security and Privacy in Public Cloud Computing.[5] In fact, the U.S. Government and political campaigns have relied on the company's services as well, including Cloudflare's CDN.[6]

(2) Open-Source Set-Top Boxes

Another example of commenters raising concerns about generalized technology is the MPAA's characterization of customizable, open-source set-top boxes utilizing the Kodi multimedia player application along with websites that allegedly "enable one-click installation of modified software onto set-top boxes or other internet-connected devices."[7] Unscrupulous vendors selling general-

recent years to develop reasonable, voluntary measures to prevent sites focused on copyright infringement from using their services.").

[3] *See e.g.*, Cloudflare, *Project Galileo*, https://www.cloudflare.com/galileo/ (last accessed Oct. 16, 2017).

[4] Miles Tracy et al., *Guidelines on Securing Public Web Servers*, Special Publication 800-44, Version 2 (National Institute of Standards and Technology, Sept. 2007), at 8-12, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf.

[5] Wayne Jansen & Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, Special Publication 800-144 (National Institute of Standards and Technology, Dec. 2011), at 13, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. *See also* NIST US Government Cloud Computing Technology Roadmap Volume III, *Technical Considerations for USG Cloud Computing Deployment Decisions*, Document NIST XXX-0XX, First Working Draft (National Institute of Standards and Technology, Oct. 31, 2011), at 71, https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_cloud_roadmap_VIII_draft_110111-v3_rbb.pdf (discussing the importance of CDNs).

[6] Cloudflare Case Study, DonaldJTrump.com, https://www.cloudflare.com/case-studies/trump/ (last accessed Oct. 16, 2017).

[7] MPAA Comments at 3.

purpose devices preloaded with software whose function is to infringe content or circumvent technological protection measures (TPMs) are an appropriate target for enforcement activities.

These enforcement activities should focus on the infringers themselves, however, not a general-purpose technology, such as an operating system for set-top boxes, which may be used in both lawful and unlawful ways. Open-source software designed for operating a home electronics device is unquestionably legitimate, and capable of substantial noninfringing uses. Indeed, even the MPAA itself notes that "Kodi is not itself unlawful," and that the media player application itself "does not host or link to unlicensed content."[8] E-commerce provider Alibaba also notes that these set-top box devices can be legal.[9]

The offering of devices modified to infringe, or with the clear aim of intentionally inducing infringement, may well violate local copyright laws, where the copyright law of the jurisdiction in question prohibits TPM circumvention or inducement. In these cases USTR should take care to differentiate between lawful open-source technology and a minority of users and businesses who employ that technology for infringement.

Respectfully submitted,

Matt Schruers
VP, Law & Policy
Computer & Communications Industry Association
655 15th Street NW, Suite 410
Washington, D.C. 20005
(202) 783-0070
mschruers@ccianet.org

[8] *Id.*
[9] Alibaba Comments, ID No. USTR-2017-0015-0020, at 30.