Before the

OFFICE OF THE U.S. TRADE REPRESENTATIVE

In the Matter of

2017 Special 301 Out-of-Cycle Review of Notorious Markets

Docket No. USTR-2017-0015

Reply Comments of the Electronic Frontier Foundation

October 16, 2017

The Electronic Frontier Foundation (EFF) submits these reply comments relating to the 2017 Special 301 Out-Of-Cycle Review of Notorious Markets. EFF is a member-supported nonprofit organization devoted to protecting civil liberties in the digital world. With over 36,000 dues-paying members, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

In this reply, we respond to the comments of several industry associations regarding the role and responsibilities of Internet intermediaries with respect to enforcing copyright and trademark laws. These and similar comments, which in past years have been reflected uncritically in USTR's Notorious Markets reports, mischaracterize U.S. law and policy on the role of intermediaries in Internet communications. To the extent they affect U.S. trade policy (and domestic economic policy), these misstatements will hurt the competitiveness of U.S. businesses and undermine important technological and structural protections for free expression.

The Notorious Markets Report is developed under the auspices of the Special 301 process. As others have documented at length in previous submissions[1] and publications,[2] there are serious questions over the very legality of the Special 301 process, to the extent that it purports to be a mechanism for raising trade disputes. The WTO agreement provides:

> Members shall not make a determination to the effect that a violation has occurred, that benefits have been nullified or impaired or that the attainment of any objective of the covered agreements has been

[1] Submission of Global Health Organizations, February 15, 2011, available at http://infojustice.org/wp-content/uploads/2011/02/Submission-of-International-Health-NGOs-for-the-2011-Speical-301-Report.doc.

[2] Jagdish Bhagwati and Hugh T. Patrick (eds.), Aggressive Unilateralism: America's 301 Trade Policy and the World Trading System, pp. 113-14 (University of Michigan 1993).

> impeded, except through recourse to dispute settlement in accordance with the rules and procedures of this understanding.[3]

Under Section 306 of the Trade Act, the USTR is empowered to apply sanctions if a country fails to satisfactorily implement measures to redress the concerns it has unilaterally raised of that country in the Special 301 report. This is facially incompatible with the WTO agreement, and has only survived WTO scrutiny to date on the basis of U.S. undertakings, notwithstanding the language of the Trade Act, that the USTR would not apply such sanctions outside of WTO dispute resolution mechanisms. The WTO panel that ruled to that effect however explicitly cautioned that:

> should [the US Administration's undertakings] be repudiated or in any other way removed by the US Administration or another branch of the US Government, the findings of conformity contained in these conclusions would no longer be warranted.[4]

The Notorious Markets Report explicitly "encourages governments … to engage in sustained and meaningful efforts to combat piracy and counterfeiting,"[5] which can be understood by those governments as foreshadowing further action to be taken in the event that they do not accept the USTR's "encouragement."

In practice, even without the need for sanctions to be applied or explicitly threatened, this implicit threat has created heavy extra-legal pressure on countries to amend their intellectual property laws and policies to accord with the USTR's unilateral demands, and the result has often been to the detriment of those countries' citizens, with a very unclear benefit, if any, for the United States.

The comments of various entertainment and pharmaceutical associations regarding Internet technologies threaten particular harm to U.S. trade and speech interests.

A. Content Delivery Networks and Reverse Proxy Services

Content delivery networks, or CDNs, are services that improve the performance, security, and reliability of websites, by replicating websites' content and

---

[3] Understanding on Rules and Procedures Governing the Settlement of Disputes, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, art. 23.2, Legal Instruments – Results of the Uruguay Round vol. 31, 33 I.L.M. 81 (1994).

[4] WTO Panel, WT/DS152/R, United States—Sections 301–310 of the Trade Act 1974, available at http://www.sice.oas.org/DISPUTE/wto/tract01e.asp.

[5] USTR, 2016 Out-of-Cycle Review of Notorious Markets (December 2016), https://ustr.gov/sites/default/files/2016-Out-of-Cycle-Review-Notorious-Markets.pdf.

functionality in multiple physical locations.[6] Reverse proxy services, a similar category, are services that stand between a website host and its users, making them resistant to denial-of-service attacks that could render them inaccessible.[7] CDN and reverse proxy services are used by millions of websites, and are instrumental in allowing individuals and small businesses to reach a global audience reliably.

Comments from the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and the Entertainment Software Association (ESA) in this proceeding paint a misleading picture of CDNs and reverse proxy services. For example, RIAA describes them as services used by "pirate sites … to obfuscate their IP address, creating obstacles to enforcement against such sites."[8] MPAA repeatedly describes CloudFlare, a popular CDN and reverse proxy service, as a service that "masks the IP location of the web site." MPAA also states without evidence that a site's purpose for using a reverse proxy service is "to curb rights holders' ability to identify its precise host."

What these commenters fail to mention is that nearly *any* service that stands between a website and its users will inherently cause users to see a different Internet Protocol (IP) address than the one used by the website's own server. This is neither nefarious nor particularly difficult to circumvent, given that CDNs are well-established, largely US-based companies that respond to valid court process requesting the IP address of a website.

CDNs and reverse proxy services perform a vital role in making websites more robust platforms for speech of all kinds, and enhancing the global reach of American businesses via the Internet. While U.S. copyright law requires these services to refrain from knowingly contributing to specific copyright infringements, purposefully inducing infringement by customers, or assuming a supervisory role over customers who infringe while profiting from such infringement,[9] they are not required to seek out or police infringement by their customers,[10] nor to render alleged infringers easily identifiable by copyright holders. Pressure on these services, including from USTR, to engage in more private copyright enforcement than the law requires, risks diminishing the benefits that the services provide for U.S. trade competitiveness and for the preservation of robust free speech.

---

[6] CDNetworks, "How Content Delivery Networks Work" (April 13, 2015), https://www.cdnetworks.com/en/news/how-content-delivery-networks-work/4258

[7] "Protect Against DDoS Attack," Cloudflare, https://www.cloudflare.com/ddos/ (accessed October 16, 2017).

[8] RIAA Comments at 4.

[9] *See, e.g.*, *MGM Studios, Inc. v. Grokster, Ltd.,* 545 U.S. 913 (2005).

[10] *See, e.g., Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995),

Accordingly, USTR should decline the invitation to call out CDNs and reverse proxy services in its report. These services are not "notorious markets," nor do they have any meaningful connection to such markets, aside from providing them the same services used by millions of other websites.

B. Domain Name Registrars and Registries

The domain name system (DNS) is a global distributed database maintained by hundreds of independent entities. Its main function is to correlate domain names such as ustr.gov with numeric Internet Protocol addresses, such as 198.137.240.1, which are used to route information across the Internet. Nearly every Internet-connected device makes use of the DNS. Policies for the system are set by the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit corporation that operates under a multi-stakeholder policy process.[11] Companies known as DNS registrars perform the service of registering domain names in the system on behalf of users.[12] Registrars' practices are determined in part by contractual agreements with ICANN.[13]

The DNS is a vital part of the Internet's infrastructure, and is one of the consensus-based approaches that, by and large, allows a person to access information anywhere in the world regardless of the technology they use or how they connect to the Internet. It operates not under the mandate of any government but rather a sometimes fragile consensus among stakeholders. That consensus is maintained in part by limiting the purpose of the DNS to the narrow, technical function of associating Internet resources with human-readable names in a consistent and robust way.

In 2011, Congress considered a bill that would have required registrars to suspend domain names as a remedy for copyright and trademark infringement on websites. Reflecting in part the concerns described above, and following a broad public outcry, Congress abandoned this proposal in 2012.[14]

Some special interests, however, still seek to repurpose the DNS as a tool for furthering particular legal, commercial, and social policies. They seek to transform a domain name from a simple identifier into a license to speak on the Internet, to be granted or revoked based on various and shifting standards of good behavior,

---

[11] "What Is ICANN Policy?," https://www.icann.org/policy#what_is_policy (accessed October 16, 2017).
[12] "Information for Registrants and Registrars," https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en (accessed October 16, 2017).
[13] *Id.*
[14] "After Historic Protest, Members of Congress Abandon PIPA and SOPA in Droves," EFF Deeplinks Blog (Jan. 19, 2012), https://www.eff.org/deeplinks/2012/01/after-historic-protest-members-congress-abandon-pipa-and-sopa-droves

enforced and executed by private actors with conflicting and sometimes anti-competitive incentives.

Some of the comments in this proceeding reflect this dangerous trend. For example, the Alliance for Safe Online Pharmacies (ASOP) seeks to co-opt DNS registrars into acting as private pharmacy regulators by seeking out and suspending the domain names of websites that ASOP deems to be illegal online pharmacies.[15] While ASOP is correct that a registrar may use its own discretion to suspend a domain name when "the registrar deems such suspension is appropriate,"[16] ASOP also requests that the government direct the exercise of that discretion, stating that the failure to suspend domains "should not be tolerated" by USTR.[17]

It would be wholly inappropriate for USTR to press domain name registrars to act as enforcers of pharmacy licensing requirements or to suspend domains at the request of the pharmaceutical industry. While ASOP decries an "often long back-and-forth process with the courts"[18] required to take down a website engaged in illegal pharmaceutical sales, the solution to this problem is not to bypass due process of law by encouraging registrars to suspend domain names on their own initiative.

C. "Stream Ripping" Websites

Finally, RIAA's discussion of "stream-ripping" websites misstates copyright law.[19] Websites that simply allow users to extract the audio track from a user-selected online video are not "illegal sites" and are not liable for copyright infringement, unless they engage in additional conduct that meets the definition of infringement. There exists a vast and growing volume of online video that is licensed for free downloading and modification, or contains audio tracks that are not subject to copyright. Moreover, many audio extractions qualify as non-infringing fair uses under copyright. Providing a service that is capable of extracting audio tracks for these lawful purposes is itself lawful, even if some users infringe.[20] Such a website does not become "illegal" by earning revenue through advertising. Other activities may give rise to copyright liability, such as distributing infringing copies of video and audio recordings to third parties, but many of the sites identified by RIAA are not clearly involved in such activities.

USTR must apply U.S. law as it is, not as particular industry organizations wish it to be. Accordingly, it is inappropriate to describe "stream-ripping" sites as engaging in or facilitating infringement. That logic would discourage U.S. firms from providing

---

[15] ASOP comments at 2-3.
[16] ASOP comments at 2.
[17] *Id.* at 3.
[18] *Id.*
[19] RIAA comments at 5-8.
[20] *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

many forms of useful, lawful technology that processes or interacts with copyrighted work in digital form, to the detriment of U.S. trade.

Respectfully submitted,

Mitchell L. Stoltz
Jeremy Malcolm
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
mitch@eff.org