NISKANEN CENTER

Public Interest Comment

Submitted to the United States Trade Representative in the Matter of:

A Rebuttal to "A Request for Comment on the 2016 Special 301 Out-of-Cycle Review of Notorious Markets"

Ryan Hagemann

Technology and Civil Liberties Policy Analyst
The Niskanen Center

Submitted: October 20, 2016
Docket No. USTR-2016-2013

Executive Summary

The Niskanen Center wishes to draw the U.S. Trade Representative's (USTR) attention to a number of spurious and erroneous claims forwarded by other commentators on the *2016 Special 301 Out-of-Cycle Review of Notorious Markets*. We argue that the reference to content delivery networks (CDN) serves to misdirect attention away from web hosting services and, more importantly, individual infringers of copyright law. CDNs are not, despite suggestive claims to the contrary, web hosting providers and many possess no means of taking direct action through the "notice and takedown" provision in 17 U.S. Code § 512.

We take no position on the particular websites and foreign markets listed in the submitted comments. It may very well be the case that many, most, or all of those sites offered by other commenters are indeed guilty of copyright infringement. Our intention is simply to point out the mistaken assertion that CDNs, and the services they offer consumers, are to blame. To that end, we offer a technical illumination of the facts surrounding the operations of CDNs, and refer the USTR to the numerous benefits—from the proliferation of trust online to effective cybersecurity responses—that CDNs offer the online ecosystem.

Introduction

Copyright enforcement in the digital age is notoriously difficult, and piracy is an issue for many industry actors. These comments, however, are not concerned with the particular site listings that may constitute notorious markets. Rather, we refute the claims referencing content delivery networks (CDN) as enablers of notorious market actors.

Some commentators have intimated that content delivery networks, Internet service providers (ISP), and other companies operating in the Internet infrastructure ecosystem ought to more diligently monitor and police the content of their customers. We wish to clarify the technical limitations of CDNs operating in a non-web hosting role. These comments are meant to eliminate confusion over the role that CDNs play and why they should not be considered facilitators of copyright infringement.

Content Delivery Networks: An Overview

As noted in a white paper on CDN architecture from Akamai Technologies, a pioneer in the development of CDNs:

> *inherent limitations in the Internet's architecture make it difficult to achieve desired levels of performance natively on the Internet. Designed as a best-effort network, the Internet provides no guarantees on end-to-end reliability or performance. On the contrary, wide-area Internet communications are subject to a number of bottlenecks that adversely impact performance, including latency, packet loss, network outages, inefficient protocols, and inter-network friction.*[1]

CDN services are meant to optimize content delivery through a variety of transport mechanisms, including server load-balancing,[2] web caching,[3] and request routing.[4] Although the specious contention of some commentators that the use of a "reverse proxy functionality" is intended to provide companies and individuals illicit Internet Protocol (IP) masking services, this service is actually aimed at improving cybersecurity, protecting against theft, and boosting server performance.[5]

---

[1] Erik Nygren, Ramesh K. Sitaraman, and Jennifer Sun, "The Akamai Network: A Platform for High-Performance Internet Applications," Akamai Technologies, https://www.akamai.com/us/en/multimedia/documents/technical-publication/the-akamai-network-a-platform-for-high-performance-internet-applications-technical-publication.pdf.

[2] Load-balancing involves distributing computation across multiple computers in order to "balance" the resource "load" in order to ensure optimal response times. Server farms and cloud computing services are prime examples of server load-balancing, distributing computational workloads across multiple sources.

[3] Web caching is the process of temporarily storing information (a website's HTML code, associated images, etc.) in order to make retrieval by requesting users quicker, thereby reducing bandwidth costs, improving load times, and minimizing the amount of lag experienced by users.

[4] Request routing is the process of directing traffic to a particular "node" in the network that can more efficiently optimize the user's requested action. This assists in reducing bandwidth usage and reducing load times for web pages, among other benefits.

[5] "What is a Reverse Proxy Server?," NGINX Software, Inc., https://www.nginx.com/resources/glossary/reverse-proxy-server/.

CDNs are a new class of business; they are not, as some comment submissions to the USTR have suggested, web or content hosts or providers. Rather, CDNs operate in the digital cloud, between ISPs and web hosting services. As such, they are not in a position to engage in content take-down operations. That has not stopped some organizations from calling out various CDNs in their comments.

For example, comments filed by the Motion Picture Association of America (MPAA) note that websites involved in copyright infringement "depend on a hosting provider to make their website accessible online," and that the provider "has the ability to take websites ... offline." The comments continue by falsely claiming that:

> *Some hosting providers allow sites to hide behind a content delivery network (CDN). A CDN is typically used to effectively and efficiently deliver content to a global user base by placing servers all around the world that cache the pages of the website. One of the by-products of using a CDN is that they mask the true IP and hosting provider of a website. An example of a CDN frequently exploited by notorious markets to avoid detection and enforcement is Cloudflare. Cloudflare is a CDN that also provides reverse proxy functionality. Reverse proxy functionality hides the real IP address of a web server.*
>
> *Given 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.*[6]

The mention of CDNs in this context erroneously implies that these companies are the same as hosting providers. They are not. Nor is MPAA alone in inaccurately conflating these technologies. The Entertainment Software Association (ESA) echoed these concerns in a footnote within their own comments, mistakenly arguing that:

> *CDNs are not like Internet "backbone" service providers, which act as a mere conduit for traffic that they neither control nor request but enter into service agreements with websites to effectively ensure that the content of those sites is always available, and that site visitors enjoy an optimal user experience. Among other functions, CDNs cache copies of web pages to ensure the availability of site content in the event of web server malfunction. While CDNs are used by legitimate services, infringers may make specific use of these services both to hide true hosting information (i.e., public registries reference only the CDN, and not the actual host cached by the CDN), and to speed the transmission of large files, such as infringing copies of games.*[7]

---

[6] Comments of the Motion Picture Association of America, Re: Request for public comment on the 2016 Special 301 Out of Cycle Review of Notorious Markets. Docket No. USTR-2016-2013, Submitted October 7, 2016, *available at* https://www.regulations.gov/document?D=USTR-2016-0013-0007.

[7] Comments of the Entertainment Software Association, Re: 2016 Special 301 Out-of-Cycle Review of Notorious Markets: Request for Public Comments, 80 Fed. Reg. 175 (August 25, 2016), Submitted October 7, 2016, *available at* https://www.regulations.gov/document?D=USTR-2016-0013-0010.

In fact, however, CDNs actually *are* far more akin to "Internet 'backbone' service providers" than web hosting services. Based on the services CDNs provide, an OECD report from April 2010 clearly intimates they are just as much a functional Internet intermediary as an ISP.[8] Nonetheless, the Recording Industry Association of America (RIAA) mimicked the same claims as ESA and MPAA in its own comments, pointing out that:

> *more sites are now employing services of Cloudflare, a content delivery network and distributed domain name server service. BitTorrent sites, like many other pirate sites, are [increasingly] turning to Cloudflare because routing their site through Cloudflare obfuscates the IP address of the actual hosting provider, masking the location of the site. The use of Cloudflare's services can also act to frustrate site-blocking orders because multiple non-infringing sites may share a Cloudflare IP address with the infringing site.*[9]

Like MPAA, RIAA also calls out Cloudflare as essentially contributing to copyright infringement. Although ESA's comments do not reference Cloudflare in particular, their footnote goes on to suggest what MPAA and RIAA presumably want from CDNs: "to join ISPs, search engines, payment processors, and advertising services that have successfully collaborated with rights holders in recent years to develop reasonable, voluntary measures that prevent sites focused on copyright infringement from using their services."[10] Yet even a cursory examination of the services offered by Cloudflare's CDN makes it clear that it is already engaged in such efforts:

> *Cloudflare **is not a web hosting company and we have no way to remove content from a site**, but we do comply with valid copyright complaints if we receive specific proof of the complaint from the copyright holder and/or authorized agent for the copyright holder. When presented with a valid complaint we can provide who the web hosting provider is for the site in question.*[11] [emphasis added]

Cloudflare, like other CDNs, sits between ISPs and website owners—an intermediary cloud-based service provider that offers defences against malicious cyberattacks and optimizes user experience online.[12] **It is not a web hosting service, and cannot perform takedown operations.** Although this may not be the case with all companies providing CDN services, Cloudflare does not have the functional capabilities to respond to the "notice and takedown" provision of the Digital Millennium

---

[8] "The Economic and Social Role of Internet Intermediaries," *Organization for Economic Co-operation and Development*, April 2010, *available at* https://www.oecd.org/internet/ieconomy/44949023.pdf.

[9] Comments of the Recording Industry Association of America, re: Docket No. USTR-2016-2013, Submitted October 7, 2016, https://www.regulations.gov/document?D=USTR-2016-0013-0012.

[10] Comments of the Entertainment Software Association, Re: 2016 Special 301 Out-of-Cycle Review of Notorious Markets.

[11] "How do I file a DMCA complaint?," Cloudflare Support, https://support.cloudflare.com/hc/en-us/articles/200167716-How-do-I-file-a-DMCA-complaint-; Also see *Terms of Service*, Section 16: DMCA and Abuse Reports, https://www.cloudflare.com/terms/. ("Cloudflare is a pass-through network and, at most, caches content for a limited period in order to improve network performance. Cloudflare automatically removes content from our caches when it has been removed from our customer's origin web server. Cloudflare is not a hosting provider and has no way of removing abusive content on third party hosting services.")

[12] "How does Cloudflare work?," Cloudflare Support, https://support.cloudflare.com/hc/en-us/articles/205177068-Step-1-How-does-Cloudflare-work-.

Copyright Act (DMCA), 17 § U.S.C 512(c).[13] This is not within the technical purview of a CDN like Cloudflare or other CDNs, such as Akamai Technologies.[14]

The RIAA and MPAA comments are also flawed in that they treat all CDNs as one technology, which they are not. Although these comments specifically reference Cloudflare, the CDN ecosystem is quite broad.[15] Case-by-case analysis is important from a regulatory economics perspective, as the imposition of liability in such an environment must be weighed against not only the costs of doing so, but compared to the alternatives available to the individuals actually engaging in infringement.[16] That is to say that CDNs do not provide a novel or unique means by which nefarious actors might engage in copyright violations. Indeed, this is a relatively mature and robust marketplace, with many different actors providing services to a wide range of market actors. If an attempt to impose DMCA or other copyright policing responsibilities on CDNs were pursued, it should be done on a case-by-case basis. However, the Niskanen Center would argue that no such justification can reasonably find that CDNs ought to be designated as notorious markets, and therefore should be treated with the same intermediary liability protections as other Internet infrastructure providers.

There are many benefits of utilizing CDNs, not least of which are the significant cost savings on storage and bandwidth when compared to central server streaming networks.[17] Whatever benefits some actors participating in notorious markets may reap from CDN services, the mere possibility of a technological tool being used for ill is not justification enough for it to be held liable for the actions of

---

[13] 17 U.S. Code § 512 - Limitations on liability relating to material online *available at* https://www.law.cornell.edu/uscode/text/17/512. (In order to "remove, or disable access to, the material that is claimed to be infringing," the copyright-protected work in question must reside on a system or network that is "controlled by or operated by or for" a website operator.)

[14] "Akamai DMCA," https://www.akamai.com/us/en/privacy-policies/copyright-and-other-notices/akamai-dmca.jsp. ("Please note, Akamai does not review, manage, or otherwise control content creation by our customers. We provide content delivery acceleration services to speed the delivery of content from websites operated by our content provider customers to end users' browsers. Requesting Akamai to take down content will not permanently resolve content being delivered from content publisher's origin. For permanent resolution, we strongly recommend making your complaint known to the content publisher directly.")

[15] Other notable CDNs include Akamai Technologies, Google Cloud CDN, Amazon CloudFront, and Microsoft Azure, as well as a wide range of other companies.

[16] Ronald J. Mann and Seth R. Belzley, The Promise of Internet Intermediary Liability, 47 Wm. & Mary L. Rev. 239 (2005), http://scholarship.law.wm.edu/wmlr/vol47/iss1/5. (Although Mann and Belzley argue for increasing the responsibilities of Internet intermediaries in policing content infringement, they point out that any regulatory regime that attempts a "gatekeeper liability" model is bound to run into serious problems if the market is robust enough to accommodate many firms: "Thus, for example, if the sole effect of the regulation of a particular intermediary will be to motivate illicit actors to shift constantly to ever more elusive intermediaries without effecting the underlying misconduct, then the regulation's costs are likely to be a total loss. This suggests that the central factor in assessing the best regulatory strategy must be the market structure of the various intermediaries: intermediaries with sufficient market power to prevent illicit actors from moving to substitutes are better targets than those for whom ready substitutes exist. … the point is simply to emphasize that a strategy utilizing intermediaries makes sense only in contexts where the inevitable costs can be balanced against benefits in real reductions rather than in relocations of misconduct.")

[17] Cloudflare customer case studies (https://www.cloudflare.com/case-studies/); Google Cloud CDN customer case studies (https://cloud.google.com/customers/); Akamai Technologies customer testimonials (https://www.akamai.com/de/de/solutions/industries/cdn-and-cloud-services-for-startups-case-studies.jsp); Amazon CloudFront CDN customer testimonials (https://aws.amazon.com/cloudfront/?nc2=h_m1).

users.[18] As online content becomes more interactive and bandwidth-intensive, a more distributed network will increasingly become the most architecturally beneficial approach to optimizing user experience and services.

It is also worth noting that services that provide proven cybersecurity protection, whether through encryption or other means, help foment the proliferation of trust online. Without trust in the online ecosystem, e-commerce and the digital economy would collapse.[19] As a result, the many cybersecurity benefits of CDN cannot be ignored.[20] Increased cybersecurity and trust ultimately translate to greater certainty and investment in innovation. CDNs play a positive role in fomenting innovation, but can only be effective market contributors if the legal and regulatory landscape communicated stability and certainty. As David Post and others discussed in their amicus brief in *Viacom v. YouTube*:

> *Website operators and other providers of innovative online services have a clear and straightforward set of ground rules to follow, allowing them to conform their operations to the law and, thereby, to avoid the specter of potentially crushing liability. At the same time, copyright holders, through the notice-and-takedown process spelled out in 17 U.S.C. § 512(c), have simple and cost-effective means to curtail large numbers of unauthorized and infringing uses of their protected expression.*[21]

Commenting on liability limitations for intermediary providers is slightly beyond the scope of these comments. However, it should be noted that there is a strong indication that such rules have helped enable the rise of commercial web services, user-generated content platforms, and online innovation more broadly.[22]

It is also worth pointing out the potential for unnerving precedents to be set by deputizing CDNs to monitor, police, and ultimately arbitrate the content of their users. Such a situation holds the potential to chill free speech online, reduce online security, diminish trust amongst Internet users, and curtail significant economic activity and potential innovation.[23] In addition, by focusing on CDNs, the true sources of infringement—site operators whose piracy efforts ought to be the focus of these comments—go unaddressed.

---

[18] Stacy L. Dogan, "'We Know It When We See It': Intermediary Trademark Liability and the Internet," 2011 Stan. Tech. L. Rev. 7, *available at* http://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/dogan-intermediary-trademark-liability.pdf. ("As long as a technology has a significant non-infringing application, its manufacturer should be protected without regard to its intent.")

[19] Ryan Hagemann and Josh Hampson, "Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption," Niskanen Center, November 9, 2015, https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

[20] Nygren, et. al., "The Akamai Network," p. 16.

[21] Brief of Amicus Curiae in *Viacom Intl. Inc. v YouTube Inc.*, Case 10-3270, Document 312, (Aptil 7, 2011), a*vailable at* https://www.scribd.com/document/109867487/Final-Law-Professors-Brief-As-Filed-Viacom-v-YouTube

[22] Cynthia Wong, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," Center for Democracy and Technology, April 2010, https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf.

[23] Giancarlo F. Frosio, "Digital piracy debunked: a short note on digital threats and intermediary liability," Internet Policy Review, Vol. 5, Issue 1, March 23, 2016, http://cyberlaw.stanford.edu/files/publication/files/Internet%20Policy%20Review%20-%20Digital%20piracy%20debunked-%20a%20short%20note%20on%20digital%20threats%20and%20intermediary%20liability%20-%202016-03-23.pdf.

Conclusion

From a purely technical angle, many CDNs cannot assist with content take-down because they lack the ability to do so. Even if they were akin to web hosting providers in possessing such abilities, however, it would still be ill-advised to seek authority to compel CDNs to engage in such actions. The economic contributions from this emerging market are rapidly growing, but could be stymied by limiting copyright infringement liability protections for CDN firms. That would undoubtedly have negative effects for innovation and economic entrepreneurship. The industry's considerable contribution to cybersecurity is another benefit that should be accounted for when toying with the possibility of forcing CDNs into the role of deputized agents of copyright holders.

Companies like Akamai and Cloudflare already commit to abiding by 17 U.S. Code § 512 in passing along notifications of potential copyright infringement. Expecting broader assistance to police alleged copyright infringement is unreasonable. The claims offered by content industry trade groups—that CDNs are not entitled to intermediary liability protections—is an erroneous reading of the the technical capabilities and operations of CDNs. Any effort to expand enforcement obligations by USTR to these CDN companies can only harm the health of the online ecosystem; it would chill free speech, cripple innovation of an evolving Internet architecture, and serve to make millions of websites less secure.

While it is certainly true that copyright holders have legitimate grievances with regards to online privacy, suggesting that CDNs should play a more active role in content policing is a risky and imprudent proposition.