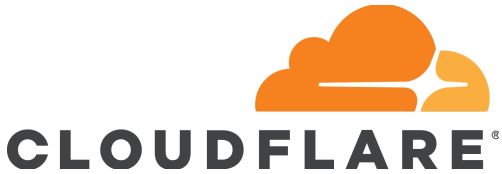

October 21, 2016

Christine Peterson
Director for Intellectual Property and Innovation
Office of the United States Trade Representative

Re: Rebuttal comments regarding the Request for public comment on the 2016 Special 301 Out of Cycle Review of Notorious Markets Docket. No. USTR-2016-2013

Dear Ms. Peterson:

I learned recently of dozens of references to Cloudflare in two October 7, 2016, letters to USTR from the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA). The letters list foreign websites suspected of illegally distributing copyrighted content and attempts to lump Cloudflare in with these suspected infringers. This came as a surprise to my colleagues and me because as we explained to you and Probit Mehta at a meeting last November, Cloudflare is not a hosting company, cannot block websites, and is not in the business of hiding companies that host illegal content.

I am writing to provide you with information about Cloudflare, its business practices, and technologies, which are generally focused on providing cybersecurity to websites. It is not an understatement to say that cyberattacks are one of the greatest single threats to economic growth, and it is almost certainly so in the United States. The Global Risks Report 2016 from the World Economic Forum notes that such attacks cost global businesses more than $445 billion in 2014 -- a number that has almost certainly increased since then -- and ranks “Cyber attacks” and “Data fraud or theft” respectively as the first and third most likely risks for North American commerce (“Extreme weather events” is second).

Cloudflare provides a service on the cutting edge of technological and business innovation in support of our goal of “building a better Internet” by providing millions of websites with the tools to make them work faster, more efficiently, and more securely. To do this, Cloudflare operates a network of roughly 100 data centers in more than 40 countries functioning as what is called a “reverse proxy.” This reverse proxy sits between our customers’ websites and the public Internet in order to protect the websites from malicious attacks. The system uses the collective intelligence of our entire network to support and immediately update our web application firewall, and it provides best in class Distributed Denial of Service (DDoS) protection, which has become an increasingly important defense in light of recent cyber attacks, including a massive attack ongoing today (Oct. 21) that has significantly interrupted service to many prominent websites, utilizing data from tens of thousands of compromised video cameras.

Cloudflare is also at the cutting edge of providing features like TLS 1.3 encryption, IPv6, and DNSSEC. Cloudflare does all of this while improving page load performance and achieving significant gains in bandwidth efficiency by answering Internet queries from data centers much closer to the end user.
In order to protect our customers, Cloudflare directs Internet inquiries directly to our cached versions

of websites at our data centers rather than the servers hosting our customers' web content. That architecture protects websites that would otherwise be under threat of direct cyber attack and threats like DDOS or ransomware attacks. Making information publicly available about the exact location of the website host would permit circumvention of our protections and allow sites to be attacked directly. There are a number of Content Delivery Networks (CDNs) and Virtual Private Networks (VPNs) that do the same thing by routing internet queries to locations other than the origin host.

Based on the success of our services, Cloudflare -- which launched in 2010 -- now provides web optimization and security services to more than four million website customers worldwide. Cloudflare protects the websites of such diverse customers as NASDAQ, Bain Capital, the Library of Congress, the band Metallica, Cisco Systems, and a number of state and national governments. Cloudflare has been recognized with multiple Tech Innovation Awards from the Wall Street Journal, and was named part of both CNBC's Disruptor 50 and Forbes' Cloud 100. Our services benefit our customers--and the billions of people who use their websites--to make the entire Internet more secure.

The submissions by the RIAA and MPAA present distorted descriptions of services that companies like Cloudflare provide. These descriptions fail to provide the USTR with an accurate description of the true intent, purpose, and value of Cloudflare's services.

Potentially even more troubling than the RIAA and MPAA's descriptions of Cloudflare's services is their complete omission of Cloudflare's efforts to address the small minority of users about which they complain. As both RIAA and MPAA are aware, Cloudflare has created a "Trusted Reporter" program to permit identification of the website host in response to complaints of abuse or infringement when the requestor has been identified as someone other than a potential cyber threat. Both the RIAA and the MPAA participate in our Trusted Reporter Program and are frequent users of the system. We are now in discussions with the RIAA on how to effectively expand the scope their involvement in that program.

Such requests are generally responded to in a matter of hours, and almost always within a business day. It is telling that neither the RIAA or MPAA complain in their submissions that Cloudflare's system fails to provide the responsive information on a timely basis. So the "obfuscation" discussed by them is more accurately described as an operation that is essential to well-functioning CDN and VPN networks, and is mitigated by the Trusted Reporter program.

Cloudflare processes thousands of infringement and abuse complaints every week. Cloudflare does not make the process of enforcing intellectual property rights online any harder -- or any easier. We follow all applicable laws and regulations. We facilitate the enforcement process for participants in the Trusted Reporter program, which provides origin IP addresses on an expedited basis to more than 40 major intellectual property rights holders and rights organizations that have been pre-cleared as non-threats by Cloudflare.

In their submissions, the RIAA and MPAA make reference to a total of 48 websites that they describe as obfuscated by Cloudflare. What they fail to mention is that the RIAA and MPAA requested the allegedly "obfuscated" information from Cloudflare for 27 of those sites and received the relevant host information in a matter of hours. Even though they were well aware of the system, they never even

requested information on the remaining 21 sites mentioned in their letters. Yet they included those sites in their submission to the USTR without attempting to use available resources to get the information.

Cloudflare provides essential services to help millions of websites defend themselves against potentially ruinous cyber attacks. At the same time, pursuant to the Digital Millennium Copyright Act (DMCA) and good commercial practices, we have set in place a reasonable and responsive method to mitigate concerns about the ability to pursue website hosts over claims of infringement. The DMCA provides the statutory solution and process for balancing the interests of copyright holders and those of internet services companies. Under its specific terms, the DMCA protects service providers like Cloudflare from monetary liability in lawsuits, which improperly attempt to co-opt an uninvolved Internet service provider into a dispute between a website operator and a copyright holder.

In light of all the information we have provided, we trust that USTR will agree with Cloudflare that complaints by RIAA and MPAA implying that Cloudflare is aiding illegal activities should have no place whatsoever in USTR's Notorious Markets inquiry. If it is helpful in any way, Cloudflare would be happy to provide any additional information, respond to any specific questions, or make ourselves available for a meeting to discuss any of this information further.

Sincerely,

Doug Kramer
General Counsel