October 25, 2021

Jacob Ewerdt
Director for Innovation and Intellectual Property
Office of the United States Trade Representative

Re: Rebuttal comments regarding the Request for public comment on the 2021 Special 301 Out of Cycle Review of Notorious Markets, Docket No. USTR-2021-0013

Dear Mr. Ewerdt,

We write in response to the request for comments published by the Office of the United Trade Representative concerning the 2021 Review of Notorious Markets for Counterfeiting and Piracy. As in previous years, a small number of rightsholder groups have mentioned Cloudflare in their responses. These responses both contain mischaracterizations about the nature of Cloudflare's services and advocate for new policy actions and approaches unrelated to "identif[ying] online and physical markets that reportedly engage in and facilitate substantial copyright piracy or trademark counterfeiting that infringe on U.S. intellectual property (IP)."[1] We believe that the continued submission of comments from rightsholder groups designed to pressure Cloudflare and other Internet infrastructure companies to take action that is neither expected nor required by U.S. law is both misguided and an inappropriate use of the Notorious Markets process.

We are submitting these comments to provide additional background on Cloudflare as well as actions we have taken over the past year to work with rightsholders, including many of those who filed comments.

I. Background on Cloudflare

[1] Office of United States Trade Representative, Request for Comments: 2021 Review of Notorious Markets for Counterfeiting and Piracy, 86 Fed. Reg. 48464 (Aug 30, 2021).

As described in past years, Cloudflare runs one of the world's largest networks, providing security, performance, and reliability services to approximately 25 million Internet properties. Cloudflare powers Internet requests for approximately 19% of the Fortune 1,000, and serves 25 million HTTP requests per second on average.

Cloudflare offers a wide variety of services to improve the security, reliability, and performance of online web properties. Cloudflare's website security services work by directing web visitor traffic to Cloudflare's network rather than directly to the website's hosting provider. Cloudflare then uses its 250 "points of presence" in more than 100 countries to screen traffic for cybersecurity risks and to cache content at the network edge in order to improve website performance. Although Cloudflare does offer certain web hosting services to a limited number of sites[2], all of the submitted responses that reference Cloudflare exclusively refer to our security and caching services.

Contrary to the comments submitted by React, this type of caching, which is designed to improve Internet efficiency, is not the same as web hosting. Indeed, the U.S. District Court for the Northern District of California recently concluded that Cloudflare's security and caching services do not materially contribute to copyright infringement, observing that "removing material from a cache without removing it from the hosting server would not prevent the direct infringement from occurring" and "[f]rom the perspective of a user accessing the infringing websites, these services make no difference."[3]

Cloudflare has long believed that tools that make the Internet faster, more secure and more reliable should be widely available, rather than restricted to the largest businesses. This is more true than ever in an era of spiking ransomware and

[2] As detailed in Cloudflare's transparency report, the number of takedown notices that Cloudflare has received for content stored on our network is exceedingly small. (See https://www.cloudflare.com/transparency/) For those requests, Cloudflare conducts notice and takedown procedures, consistent with the requirements of the Digital Millennium Copyright Act (DMCA).

[3] *See Mon Cheri Bridals, LLC v. Cloudflare, Inc.*, Case No. 19-cv-01356-VC (N.D. Cal. Oct. 6, 2021) available at https://assets.ctfassets.net/slt3lc6tev37/7gr79MdC7Wnb3zbVzJoRzP/507d581550d04e7ac7a7f71d3c0a6715/2021_10_06_-151_0-_ORDER_by_Judge_Vince_Chhabria_Den_124_Pls_MSJ_granting_133_Def_s_MSJ_Further_Case_Management__1_.pdf.

cyberattacks. Cloudflare therefore makes security and optimization services accessible, for free, through an online sign up process. This fast, easy sign up process enables access to security tools for millions of organizations that would otherwise not have access to them, from small businesses, to non-governmental organizations, to state and local election websites. By improving the overall security of the Internet and dramatically reducing bandwidth congestion, these services help the entire Internet ecosystem, not just a single website or Internet user, and serve Cloudflare's mission to help build a better Internet.

II. Cloudflare's abuse process and work with rightsholders

Cloudflare has an abuse reporting system that can be used to report copyright infringement on the millions of websites that use Cloudflare's services. To the extent that Cloudflare receives a complaint about a website using our security services, the abuse reporting process is designed to put complainants in the same position they would be if the websites at issue did not use our security services, by ensuring that rightsholders have a way to report alleged infringement to those with the capability to remove the content from the web. Cloudflare's automated abuse system passes on complaints of copyright violations to the website owner and hosting provider, enabling them to take appropriate action. At the same time, Cloudflare also responds to complaints with information about the hosting provider so that complainants can follow up directly as necessary.

Given our abuse reporting system, use of Cloudflare services does not fundamentally alter rightsholders' ability to access websites' hosting providers. To obtain hosting provider information for an infringing website, a rightsholder simply has to submit a copyright complaint through Cloudflare's abuse web form. In fact, all of the rights holders who referenced Cloudflare in their complaints also referenced the hosting providers for websites that use Cloudflare's services, demonstrating Cloudflare's cooperation in providing them access to the information they need to pursue a takedown.

While Cloudflare does not make generally available sensitive origin host IP address information for websites using its services, that is for good reason. Such information could be used, and has been used in the past, by malicious actors to circumvent Cloudflare's security services and attack the underlying websites. Although we appreciate the importance of addressing copyright infringement, we do not believe that opening a website up to cyberattack is either an appropriate or legally acceptable way to address infringement.

That said, Cloudflare does provide origin host IP addresses through its Trusted Reporter program to those entities that have proven a genuine need for the information and have adequately demonstrated the willingness and ability to secure the information and protect it from being used for cyberattack. A variety of industry groups representing a large number of intellectual property rightsholders participate in our Trusted Reporter program, including MPA, RIAA, Entertainment Software, and Federation of the Swiss Watch Industry. Requests through this program are generally responded to in a matter of hours, and almost always within a business day. Over the course of the past few years, Cloudflare has also worked with a small number of rightsholder groups to innovate on ways to speed up access to information, leveraging automation to facilitate its processes when appropriate. We look forward to continuing to develop new mechanisms to improve in this area.

Unfortunately, however, some rightsholders who have been granted access to sensitive IP information through our Trusted Reporter process have demonstrated through public Notorious Markets submissions that they do not believe they have an obligation to secure that information. This flagrant disregard for the sensitivity of the information they have been given and the commitments they made when signing up for the program does not help build trust or long-term cooperative relationships.

In addition to the information Cloudflare provides as part of our abuse reporting process, Cloudflare offers additional resources to help rightsholders investigating possible infringement. We provide information in response to appropriate legal process, such as subpoenas issued under the Digital Millennium Copyright Act, 17

U.S.C. § 512(h). Contrary to comments made by React in its submission, we do not believe it is appropriate to provide *any* third party - including a rightsholder group - with our users' sensitive personal information like "e-mail address, IP address or connected payment method information" without valid legal process. Not only would such action be inconsistent with the privacy laws of many countries, developing any process that enabled it would be ripe for abuse.

Cloudflare continues to engage in discussions with industry groups, regulatory bodies, and law enforcement to explore additional steps that we can take to address concerns about online infringement, consistent with existing legal frameworks.

III. Conclusion

The security services that Cloudflare provides improve the overall security and performance of the Internet, and do not materially contribute to copyright infringement. We believe it is time for rightsholders to shift their comments away from policy advocacy to focus instead on the physical and online markets that are the intended subject of the Notorious Markets report.

Cloudflare will continue to act responsibly and thoughtfully to assist rightsholders in a manner consistent with the services we provide. We look forward to further discussions with you as we work with stakeholders to identify ways to address online infringement.

Sincerely,

/s/ Alissa Starzak

Alissa Starzak
Vice President, Global Head of Public Policy