Dear Sir, Madam,

We write in response to statements regarding Cloudflare submitted by other stakeholders in the context of DG TRADE's public consultation on its Counterfeit & Piracy Watch List. As we expressed in our previous submissions to you, we were disappointed not to have a chance to provide input before Cloudflare was listed on the European Commission's Staff Working Document of 2018,[1] which included numerous inaccurate statements about Cloudflare. We appreciate however having been able to provide comments to DG TRADE in 2020, and again today. It is encouraging that the Commission is looking to improve the input and comment process for the Watch List with every new publication.

As an initial matter, the creation of a Watch List suggests that the European Commission is evaluating whether entities have failed to meet their legal obligations and has identified entities that are truly bad actors. Given this reality, DG TRADE must apply principled and fair legal standards in determining which entities to include on the Watch List. The Commission should not issue a report - even an informal one - that is simply a mechanism for particular stakeholders to air their grievances that entities are not taking particular *voluntary* action to meet their concerns or to advocate for new policies. The Commission's inclusion of allegations of this type on its Watch List has the potential to inappropriately suggest that the Commission endorses such actions, a view that could influence ongoing legal discussions and policy debates. Our view is that the Commission's staff document and Watch List should be limited to Commission-verified allegations of illegal behaviour, based on principled and fair legal standards.

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

Background on Cloudflare

As we explained in our previous submission to you, Cloudflare provides security, reliability, and performance services to a significant portion of the Internet. Cloudflare believes in making cybersecurity services easily accessible, offering both free and paid services that can be accessed online. The broad availability of Cloudflare's services helps mitigate the

[1] http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf

risk posed by malicious cyber activities, and improves the reliability and performance of the Internet for everyone online. This approach also helps ensure that a variety of important but underfunded organisations are protected from cyberattack, including civil society and independent journalism organisations,[2] election infrastructure,[3] and political campaigns.[4]

The ability to quickly and easily sign up for free or low-cost security services provides a huge benefit to companies and entities large and small looking to secure and optimise their websites. Altering this online sign up process, which is consistent with existing law, to require manual review of new accounts would make it impossible to offer these free services at scale, degrading the Internet experience for all users and making much of the web more vulnerable to cyber attack. The Watch List is not the appropriate place for advocacy on new policies as to what online service providers should collect on their users.

We have seen in some of the stakeholder contributions, as in previous years, a misunderstanding of how our services work and what their function is with regard to the removal of illegal content from the Internet. For instance, some of the contributions erroneously call our reverse proxy cybersecurity services and CDN services "hosting" services.

To be effective, Cloudflare's security services require visitor traffic to be directed through Cloudflare's network rather than directly to websites' origin hosts. Cloudflare does not host material through these services, however, and Cloudflare is therefore not able to remove particular pieces of content from the Internet if they are using our reverse proxy or CDN services.

In fact, a 2021 court decision from the U.S. District Court for the Northern District of California regarding CDN services, concluded, after fact-finding, 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."[5]

---

[2] https://www.cloudflare.com/galileo/

[3] https://www.cloudflare.com/athenian/

[4] https://www.cloudflare.com/campaigns/

[5] 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_Ma nagement__1_.pdf

Our abuse reporting system & cooperation with rightsholders

Because of the way our DDoS protection and CDN services work, our abuse reporting system[6] is designed to put complainants in the same position they would be if the websites at issue did not use our services, by ensuring that rightsholders and others 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. Cloudflare's approach to this issue aligns with the frameworks set forth in Europe's e-Commerce Directive and the United States' Digital Millennium Copyright Act.

Given our extensive 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[7]. 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. Indeed, many other service providers — including Content Delivery Networks, security providers, and Virtual Private Networks (VPNs) — follow a similar model of routing Internet queries to locations other than the origin host to improve security and privacy.

Cloudflare's abuse reporting system and its Trusted Reporter program also demonstrate its cooperation with rightsholders, including several that submitted comments to the consultation. For instance, while our abuse reporting process is available to everyone, in response to requests from large rightsholders, Cloudflare has built an API that enables frequent reporters to automate the submission of abuse complaints. This enables large rightsholders in need of a system that allows them to submit a large number of reports at the same time, like IFPI and the Federation of the Swiss Watch Industry, to enable automated submissions of abuse reports, in bulk quantities.

Cloudflare has also built a Trusted Reporter program, designed for large rightsholder organisations who have demonstrated a need for additional information and a capacity to

[6] https://www.cloudflare.com/trust-hub/abuse-approach/
[7] https://abuse.cloudflare.com/

protect sensitive information. Along with law enforcement agencies, our Trusted Reporter program consists of more than 40 major intellectual property rightsholders and rights organisations in Europe, including several respondents to DG TRADE's consultation such as IFPI, Federation of the Swiss Watch Industry and MPA.

In addition to the responses that all reports through our abuse web form receive, our Trusted Reporters receive origin IP addresses of the hosting provider as well. Our Trusted Reporter network allows all parties to build trust and to work collaboratively together, with the understanding that IP origin information is sensitive and can be used by bad actors in order to attack Cloudflare's security protection layer. We value the collaboration with our Trusted Reporters, and are continuously exploring ways we can work better together, and include more automation in our processes when working together with rightsholders.

Cloudflare leverages automation to facilitate its processes when appropriate, and looks forward to continuing to innovate in this space. Automation enables Cloudflare to process nearly all copyright reports within a handful of seconds following usage of our web reporting form. We have recently made additional investments in automated processes that we expect will decrease response time to abuse reports even further. Cloudflare also continues to engage in discussions with industry groups, regulatory bodies, and law enforcement around Europe to explore additional ways that we can help.

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 and websites that are the intended subject of the Watch List 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.