October 2024

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. We appreciate having been able to provide comments to DG TRADE, as was the case for previous editions of the Watch List. It is also 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, we want to reiterate our concern that many stakeholders have again approached the Watch List as an opportunity to advocate for policy changes. We would encourage the European Commission to maintain the purpose of the Watch list as a means to identify entities that are truly bad actors, and to continue to 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're also concerned that some of the comments by various rightsholders in the consultation process of the Watch List fail to recognize the value of innovative technologies that bring more security and privacy to Internet users. To encourage digital transformation and innovation in Europe, technology needs to evolve incorporating encryption, privacy, and security tools. Restricting progress and adoption of new technology tools that help protect the privacy and security of citizens operating online in order to continue the use of outdated means to combat piracy is short-sighted, and bad for Europe's long term economic development. The Commission should be exceedingly wary of either policy proposals or court cases by rightsholders that seek to restrict adoption of privacy enhancing technology, or that enable general monitoring of the private browsing activity of EU citizens solely on the premise that it is necessary to combat piracy online.

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, with more than 30% of Fortune 500 companies and millions of organisations using our services. Powered by one of the world's largest and most interconnected networks, Cloudflare blocks billions of threats online for our customers every day. Cloudflare offers a range of different services, powering websites, remote teams, APIs, mobile apps, etc.

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 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,[1] election infrastructure,[2] and political campaigns.[3]

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

[1] www.cloudflare.com/galileo
[2] www.cloudflare.com/athenian
[3] www.cloudflare.com/campaigns

infringement from occurring" and "[f]rom the perspective of a user accessing the infringing websites, these services make no difference."[4]

Our abuse reporting system & cooperation with rightsholders

Cloudflare's approach to complaints of copyright infringement varies depending on the Cloudflare services being used. For the limited situations in which Cloudflare provides hosting services, for example, Cloudflare conducts notice and takedown in response to copyright complaints.

More often, however, Cloudflare acts as a reverse proxy and CDN service, with no ability to remove content. While Cloudflare can not remove content it does not host, it plays a role in facilitating communication between rightsholders and the responsible parties to ensure that intellectual property rights are respected. Because of the way our DDoS protection and CDN services work, our abuse reporting system[5] 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 the EU's Digital Services Act 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[6]. 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.

In addition to ensuring that all rightsholders have a means to have their complaints of infringement transmitted to hosting providers, Cloudflare has built a Trusted Reporter Program to provide additional information to large rightsholder organisations and law enforcement

---

[4] 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

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

[6] https://abuse.cloudflare.com/

agencies (LEA) who have demonstrated a need for additional information and a capacity to protect sensitive information. In response to complaints of abuse or infringement, Trusted Reporters get access to the origin IP address of a website, information which could be used for a cyberattack, in addition to information about the website's hosting provider. Cloudflare has on-boarded over 200 such organisations and agencies into the Trusted Reporter Program, including several respondents to the Watch List consultation[7].

Additionally, Cloudflare has leveraged automation to expedite both the intake of abuse reports and Cloudflare's response. Cloudflare's automation enables us to respond to nearly all copyright reports within a handful of seconds following usage of our web reporting form.

Based on conversations with rightsholders, Cloudflare developed an API that enables them to automate their submissions to Cloudflare's reporting form. The API allows larger rightsholders to send abuse reports to Cloudflare in an automated way without having to enter relevant information manually into Cloudflare's abuse form. Over 100 participants in the Trusted Reporter Program are making use of the API abuse reporting form.

In addition to our abuse process, Cloudflare has automated mechanisms to limit our free services from being used to stream content online. Our free services are not intended to stream content, and we are continuously improving automated tooling that helps to identify those customers who serve video or streaming content and are thereby violating our terms of service. While these tools are designed to prevent unauthorised streaming in general, not any particular type of content that might be streamed, these efforts should have the additional benefit of addressing the streaming of infringing material.

Cloudflare continues to engage in discussions with rightsholders industry groups, regulatory bodies, and law enforcement around Europe to better understand their concerns and improve systems to address the risk of copyright infringement. Cloudflare also collaborates with LEA in cases involving large-scale piracy or other serious intellectual property crimes. However, Cloudflare emphasises the importance of following legal procedures, ensuring that any requests from law enforcement are properly vetted and in line with legal standards to protect both the rightsholders and the rights of their customers.

A new tool for rightsholders: Cloudflare's AI Audit

Cloudflare has also found new ways to cooperate with rightsholders: On September 23, Cloudflare released a set of tools to make it easy for site owners, creators, and publishers to take back control over how their content is made available to AI-related bots and crawlers[8]. Site owners have lacked the ability to determine how AI services use their content for training or other purposes. With the new AI Audit tools, Cloudflare customers can now audit and control how AI models access the content on their site.

[7] Note that Cloudflare's Trusted Reporter program, which it provides in its discretion to assist rightsholders with regard to websites using Cloudflare's pass-through services, is not in any way related to the DSA's trusted flagger requirement, which relates to online platforms.
[8] https://blog.cloudflare.com/cloudflare-ai-audit-control-ai-content-crawlers/

We think that sites of any size should be able to determine how they want to be compensated for the usage of their content by AI models. Not everyone has the time or contacts to negotiate deals with AI companies. Up to this point, only the largest publishers on the Internet have the resources to set those kinds of terms and get paid for their content. Our recent announcement therefore previews new features which will give site owners the tools to set prices, control access, and capture value for the scanning of their content.

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.