Cloudflare Response to Call for Evidence on Combating online piracy of sports and other live events – assessment of the May 2023 Commission Recommendation

Table of Content

I. Introduction

Cloudflare is a leading connectivity cloud company that runs one of the world's largest networks, providing security, performance, and reliability services to millions of Internet properties, such as websites, networks and other applications online. Cloudflare powers Internet requests for more than 36% of the Fortune 500, and serves over 78 million HTTP requests per second on average. Cloudflare interconnects with approximately 13,000 networks globally, including major Internet Service Providers (ISPs), cloud services, and enterprises.

Cloudflare's security services work by directing traffic from the end-user to Cloudflare's network rather than directly to a hosting provider or internal network. Cloudflare then uses its "points of presence" in more than 330 cities in over 125 countries to screen traffic for cybersecurity risks and to cache content at the network edge in order to improve reliability and performance. Cloudflare also offers a global DNS resolver, 1.1.1.1., which individuals can use to navigate the Internet more securely and privately, and a developer platform that developers can use to build applications on Cloudflare's edge network.

To further our mission to "help build a better Internet," Cloudflare makes many of these cybersecurity and performance services widely available for free or at a low cost. Our free and low cost services to protect websites and applications from malicious cyberattacks are used around the globe.Our customers include every type of organization, from Fortune 500 companies and government institutions to small businesses, non-governmental organizations, and personal blogs. We also have a variety of initiatives, such as Project Galileo, that focus on providing more sophisticated cybersecurity tools to support nonprofit organizations and other organizations vulnerable to cyberattack. The result of all of the above is that we provide our services at a very significant scale, for tens of millions of domains: nearly 20 percent of all global websites use Cloudflare's network.

We welcome the opportunity to respond to the European Commission's Call for Evidence on the assessment of the May 2023 Commission Recommendation on combating online piracy of sports and other live events ('the Recommendation"). Further to our submission in February 2023 to the European Commission's Call for Evidence on Combating Online Piracy of Live Content, we bring your attention to a number of worrisome developments in multiple EU Member States. In particular, we call out misguided efforts by rightsholders to pursue network blocking measures that impede the rights of EU citizens to access lawful content and services.

This submission describes ongoing efforts in Member States to introduce blocking measures that have frequently been poorly targeted and prone to causing significant collateral damage to legitimate users of the Internet. We also outline the risks of disproportionate and harmful outcomes associated with rightsholders' proposals for legislative change, as well as minimum safeguards that should be in place before any blocking is allowed. Finally, we suggest an alternative way forward for policymakers, network providers and rightsholders to collaborate on non-legislative solutions that would more effectively combat piracy at its source.

II. Rightsholders' efforts to combat online piracy increasingly impinge on European citizens' rights and access to the Internet

Over the past two years, we have witnessed disproportionate and damaging efforts by rightsholders to use blocking measures to tackle piracy online, particularly in relation to unauthorized live streaming of sports. Pressure from these rightsholders to further their commercial interests has led some European national governments to implement problematic and imprecise legal mechanisms to tackle online piracy. These efforts often lack due process and result in far reaching negative consequences for European Internet users.

The Recommendation rightly emphasizes the importance of safeguarding applicable EU laws in addressing online piracy and advocates for the deployment of tools that are transparent, accountable, and proportionate. However, transparency, accountability and proportionality are not what we have observed in practice. Instead, rightsholders have frequently gone beyond the scope of the recommendation, pushing for harmful blocking mechanisms that have resulted in unintended collateral damage, including service outages and significant disruption of access to lawful content and tools.

A. Legislative and administrative measures have resulted in extensive collateral damage

Over the past two years, Member States such as Italy and Spain have implemented legislative frameworks that have enabled rightsholders to pursue network blocking measures that lack oversight and due process. These have included poorly targeted, judicial and administrative blocking mechanisms authorising IP address blocking that have led to foreseeable and extensive collateral damage for both network services and Internet users.

As we outline in detail here, the blocking of an IP address to attempt to block access to a website raises serious risks of overblocking because most domains are on shared IP addresses with many other domains. An IP address is not a good identifier for a particular domain because the domain can be available on any IP address, on multiple or many IP addresses simultaneously, and on a set of IP addresses that can change at any time. In the network of a large cloud provider, any single IP address may represent thousands of servers and can have even more websites and services behind it. Blocking one IP address, thus can render thousands, tens of thousands, or even hundreds of thousands of domains unreachable. It is important to underline that a 2020 ruling from the European Court of Human Rights concluded that it is improper for a government to issue orders that result in the blocking of sites that are not targeted.[1]

Member State initiatives are summarized below.

[1] *Vladimir Kharitonov v Russia*, No 10795/14 (ECtHR, 23 June 2020)

Italy: Italy's Piracy Shield grants rightsholders the ability to direct participating Internet service providers (ISPs) to block allegedly infringing content within 30-minutes of notification, without regulatory supervision or transparency. In February 2024, this resulted in a block on a Cloudflare IP address that rendered at least tens of thousands of non-targeted websites unavailable for Italian users. In October of the same year, the blocking of the domain "drive.usercontent.google.com" denied access for Italian consumers and businesses to Google Drive for over 12 hours. In both of these instances Internet users, small businesses and website owners conducting lawful activity suffered disruption and economic damage from the blocks. The blocking included no transparency over what entities were blocked, no legal description of why they were blocked, and no mechanism to contest the blocks as unlawful.

This system violates fundamental tenets of EU law, and official complaints about it have been made to the European Commission. The law that established the Piracy Shield not only led to overblocking on a massive scale, but also violated several Treaty provisions, the Charter of Fundamental Rights, Directive (EU) 2015/1535 (TRIS procedure), Regulation (EU) 2015/2120 (Open Internet Regulation), and Regulation (EU) 2022/2065 (Digital Services Act).

Spain: We have seen similar rightsholder efforts and effects in Spain. LaLiga, the country's premier football league, along with Internet Service Providers that had purchased the right to broadcast LaLiga's content, obtained a blocking order from Barcelona Commercial Court No. 6 that required Spanish ISPs to block access to IP addresses belonging to a number of cloud providers, including Cloudflare, that LaLiga alleged were linked to the unauthorized broadcast of its matches. In seeking this order, LaLiga did not inform the court that the IP addresses they were proposing to block were shared among thousands of websites and that blocking these IP addresses would inevitably lead to millions of Spanish users being blocked from accessing thousands of non-targeted websites. LaLiga secured the blocking order without notifying the implicated cloud providers, while knowingly concealing from the court the predictable harm to the general public. This blunt approach not only demonstrates a fundamental misunderstanding of how the Internet works, it also raises significant questions about compliance with the European Union's Open Internet Regulation.[2] A Spanish parliamentarian has since spoken out about these egregious acts and has proposed a parliamentary declaration in opposition to them.

Following this incident, Cloudflare moved the Barcelona court to annul its December 2024 order permitting the overblocking by LaLiga and Spanish ISPs, and argued that LaLiga misrepresented that there would be no collateral damage from the IP blocking efforts and that disproportionate blocking measures are illegal. The court nonetheless ruled against Cloudflare on the basis that Cloudflare was not directly subject to the original order, without addressing the

[2] In 2022, a coalition of copyright holders in Austria secured a court order requiring local Internet Service Providers to block 11 IP addresses associated with Cloudflare. The incident triggered a formal complaint from ISPs, who escalated the matter to Austria's independent telecoms regulator, the Telecommunications Control Commission (TKK). In 2023, after a detailed investigation, TKK concluded that IP-based blocking was disproportionate and violated both net neutrality regulations and freedom of expression. Further to the case being referred to the European Court of Justice (ECJ), the TKK's ruling was deemed final and binding, setting a precedent that reinforces legal limits on indiscriminate technical enforcement.

significant harm to Cloudflare, its customers, innocent businesses and organizations, and Spanish citizens caused by LaLiga's blocking efforts. That ruling includes neither a remedy for those harmed by overblocking nor a legal mechanism to remediate the blocking of thousands of non-targeted websites. Cloudflare has now filed an appeal to the Spanish Constitutional Court to challenge the order and establish that LaLiga's disproportionate blocking efforts are unlawful.

France: the French Government is currently considering similar legislative actions aimed at real-time blocking.[3] A new legislative proposal would enable rightsholders to report alleged infringing sites to the regulator Arcom with the expectation that access to unauthorized streams will be blocked in real-time during live sports broadcasts. If implemented in a similar manner to Italy and Spain, giving full discretion without oversight to rightsholders with a commercial interest and a lack of public accountability, this mechanism will replicate the mistakes seen in Italy and Spain, with serious repercussions for innocent Internet users and businesses.

B. Extending piracy enforcement to broader Internet infrastructure - DNS resolvers and VPNs - is misguided for combating online piracy

Despite numerous overblocking incidents, certain EU Member States continue to escalate their efforts in an attempt to restrict access to online content. Because the Internet is designed to be global and redundant, with many possible paths to the same content, blocking by network providers is highly unlikely to prevent all access to that particular content. The only way to prevent access to content definitively is to remove it at the source (i.e. at the hosting level), through processes like notice and takedown. Nonetheless some Member States, frustrated with the reality that a determined user has many paths to access content online, have taken increasingly aggressive measures to expand blocking orders beyond local ISPs.

One part of underlying Internet infrastructure that is now being targeted is the Domain Name System (DNS), which operates like a global phone book for the Internet. DNS links particular domains to the IP addresses where the content can be found online: it is a global Internet resource that is core to the structure of the Internet. Hundreds of thousands of operators around the world operate DNS resolvers that help users looking to browse the Internet with the correct IP addresses for the sites they want to visit. DNS resolvers can be operated by local ISPs solely for their users, by other organisations (like Cloudflare) that allow third parties around the world to access them (known as "public" resolvers), by organizations like virtual private network (VPN)

[3] France is considering its own draft bill on *the management and financing of professional sport*, which mandates the development of an automated system developed by Arcom to block access to unauthorized streams in real-time during live sports broadcasts. Rightsholders will provide the identification data of illicit services via the automated system (even if these have not yet been identified as of the date of the court order being issued). The automated system will send the data to those parties subject to the order so they can immediately carry out the necessary measures.

providers that integrate DNS resolution into their products, or even by individual technically-minded users.

The DNS is sometimes used for blocking, by either not returning any IP address or returning an incorrect IP address when a user requests the IP information for a restricted domain. Blocking applied to an ISP-owned DNS resolver will have a geographically restricted effect, since an ISP typically only serves users in one country. In contrast, public DNS resolvers or VPN providers operate globally. Applying a DNS-based block to a public DNS resolver or VPN would therefore mean either blocking the relevant domain for all users of the public resolver in all countries, or building a tool to identify the location of a user in order to apply appropriate blocks, with additional cost, latency, privacy, and technical challenges.

Despite this distinction, an increasing number of rightsholders and EU Member States have expanded their blocking efforts beyond ISPs and attempted to compel VPNs and global DNS resolvers to implement blocking measures. These actions are often directed at service providers that are neither based in, nor regulated by, the issuing Member State, and lack the technical tools to apply blocks in a geographically limited way. The courts and regulators in these Member States have also not required any proof demonstrating that a significant number of users in the country are actively using these services to access the content before expanding blocking obligations to these providers.[4]

Italy: The requirements in the Italian 'Piracy Shield' to block access to pirated content within 30 minutes initially only applied to Italian ISPs, whose users were guaranteed to be within Italy. More recently, however, Italy's AGCOM approved expanding the scope of the law to VPN and DNS providers. This expansion failed to consider that these providers operate their services globally, not exclusively in Italy, and that many of them are neither based in Italy nor subject to Italian jurisdiction.

France: Similar developments are taking place in France, which saw Canal+ take successful legal action against ProtonVPN, NordVPN, ExpressVPN, Surfshark, and CyberGhost, with the aim of extending blocking orders to VPN providers. This follows a similar French court order from June 2024, compelling three global public DNS resolvers (operated by Google, Cloudflare and Cisco) to block content. The court issued the blocking order despite the fact that many of the parties did not have tools to block in a georestricted way and having ample evidence that the impact on piracy would be minimal.

[4] The Internet relies on the idea that the DNS serves as an authoritative and reliable source of truth for information about where content is hosted online. A user who types google.com or commission.europa.eu into a browser expects to be taken to those sites, not to an alternative site identified by a government. Sending the wrong IP address in response to a DNS request is generally seen as a cyber attack, used by cybercriminals and malicious foreign actors for phishing and other cyber threats. Governments' mandating infrastructure providers to alter information about where content is hosted online, particularly for services that operate globally, undermines users' trust that it is operating effectively and as originally intended.

Belgium: In April 2024, Belgium followed suit, ordering the same three global DNS providers to block access to hundreds of alleged infringing websites or face fines of €100,000 euros per day. Cisco has, as a result, pulled its DNS services from both countries.

Extending blocking mandates to core Internet infrastructure providers to address the root problem of piracy for rightsholders, indiscriminately restricts access to services for all users. In addition, rightsholders have not been required to demonstrate that such orders would have a measurable impact on piracy, even though evidence suggests that only a small fraction of local Internet users rely on alternative DNS providers or VPNs to access infringing content. This raises serious questions about the need for and proportionality of such an approach. Imposing a mandate that a wide array of providers must alter core Internet technology to accommodate individual Member State demands undermines the open, global, and interoperable Internet.

III. Additional legislation is not going to solve the issue of piracy and will further delay existing solutions

Rightsholders' calls for new legislative measures—potentially including the reopening of the Digital Services Act (DSA)—risk duplicating existing legal frameworks and introducing an additional layer of complexity to an already intricate digital ecosystem. Such overreaching regulatory interventions not only undermine the coherence and effectiveness of current laws, but also threaten the openness of the Internet and weaken essential legal safeguards designed to protect fundamental rights and digital innovation.

While rightsholders argue that the DSA is not meeting their objectives in combating illegal live streaming, they have largely failed to make effective use of the mechanisms it provides. Instead, their efforts have focused on litigating against intermediaries and pressuring policymakers for disproportionate measures.

A. New legislative measures would be premature and disproportionate

The Digital Services Act (DSA) represents a carefully balanced and horizontal framework that seeks to ensure the effective removal of illegal content while safeguarding freedom of expression and access to information for platform users and the wider public. This is the right and proportionate approach. Importantly, the DSA correctly identifies hosting providers as the appropriate actors to take action against illegal content, given their direct proximity to and control over the content in question.

Proposals suggesting that intermediaries such as Internet Service Providers (ISPs) or network service providers—who have neither visibility into nor control over the content transmitted across their networks—should actively monitor or police content are fundamentally at odds with the DSA's principles. Such measures would not only conflict with longstanding European privacy law but also set a dangerous precedent that undermines legal certainty, user rights, and the open nature of the Internet.

Furthermore, the DSA is still in the early stages of implementation, and its full impact has yet to be realised across the European Union. Given the complexity of the Internet ecosystem and the need for all 27 Member States to implement its provisions consistently, rightsholders should recognise that both the European Commission, national governments and regulators require time to fully operationalise these obligations. Indeed, the European Commission recently referred five Member States - including Spain - to the European Court of Justice for failing to effectively implement the DSA. Rightsholder requests to modify the DSA at this early stage or create new requirements related to Trusted Flaggers programmes before all Member States have even fully empowered their national Digital Services Coordinator are premature and will result in even less oversight over existing processes.

B. Rightsholder requests to leverage the Trusted Flaggers programme set a dangerous precedent

Certain rightsholders have called for the Commission to reconsider the criteria for Trusted Flagger status under Article 22 of the DSA. Under the DSA, the concept of Trusted Flagger applies only to online platforms, with the understanding that online platforms have the ability to serve as a potential check against designed Trusted Flaggers who submit "insufficiently precise, inaccurate or inadequately substantiated notices."[5] Additionally, Article 22 includes a number of other safeguards, including mandating that Trusted Flaggers prepare transparency reports and comply with requirements to submit notices "diligently, accurately and objectively."

Rightsholders have called for expansion and loosening of the Trusted Flagger Programme. Such an expansion is unnecessary and inappropriate. A broader Trusted Flagger Programme that allows for on demand network blocking of illegal streaming without additional oversight, for example, would not have the many safeguards built into the DSA to protect human rights. Italy's Piracy Shield mechanism has demonstrated that there are serious risks associated with such an approach for Internet users, given its lack of due process, transparency, accountability and remedy. Rightsholder requests to block IP addresses and domain names alleged to be *"predominantly"* used for hosting or transmitting copyright-infringing content have consistently resulted in the blocking of thousands of nontargeted domains, demonstrating that there has been little or no verification of the requests' accuracy. Rightsholders have also made no effort to be proportional about what types of intermediary services should be subject to blocking orders, attempting to extend them to all possible intermediaries, regardless of whether such intermediaries have either a significant number of users or a presence in the Member State. Efforts that have such a significant likelihood of affecting third parties require oversight and means of redress. Additionally, regulators have not held rightsholders accountable for overblocking, notwithstanding the damage it causes to Internet users and lawful businesses whose content is blocked.

Obligations around trusted flagger programmes should be limited to online platforms that have DSA content moderation requirements. Extending obligations around Trusted Flagger

[5] Digital Services Act, Article 22(6).

programmes to enable third parties who wish to impose arbitrary blocking measures on intermediary services—such as ISPs or network infrastructure providers that have no visibility into or control over the content—would be inappropriate and potentially harmful. Enforcement efforts should focus on removing illegal content at its source, rather than disrupting access through intermediaries that lack the means to assess the legality of the content in question.

Expanding the DSA's obligations in Article 22 beyond their intended scope would undermine the legislations' balanced framework and pose unnecessary risks to the ability of Europeans to access lawful content and tools online, as well as the openness and integrity of the Internet.

C. Extending Know Your Business Customer (KYBC) provisions is inappropriate

Rightsholders have called for an expansion of Article 30 of the DSA, advocating for Know Your Business Customer (KYBC) requirements to apply beyond platforms facilitating consumer contracts and to extend to all online intermediaries. However, there are no material changes in the online environment that would justify revisiting the Commission's original, well-considered decision to limit these obligations to a specific category of digital services. In addition, many online intermediaries serve consumers as well as businesses, meaning that such an extension could alter the requirements beyond business customers into mandatory collection of personal information.

Moreover, it is well established that the collection of customer data is largely ineffective in deterring bad actors. Even in the highly regulated financial services sector—often cited as a model for KYBC regimes—these requirements have proven to be overly burdensome, to deter legitimate customers, and to have limited effect in addressing illicit activities. Extending such obligations indiscriminately across the entire digital ecosystem would introduce significant compliance costs and additional friction without delivering meaningful results.

Specifically, the collection of customer identifying information for network services, would do nothing to slow down criminal organisations who can easily evade such requirements.[6] Conditioning the provision of online services on the disclosure of such information would in fact restrict access to necessary services for those who most need them, and distract service providers from efforts better calculated to achieve results. Intermediary services such as VPNs and proxies, for example, are widely used to protect free expression, particularly in countries with authoritarian regimes. Onerous regulation of services that are integral to communication is not only bad policy, it is a clear violation of privacy and freedom of expression that creates an apparent conflict with Articles 7, 8 of the EU Charter of Fundamental Rights and Article 10 of the European Convention on Human Rights (ECHR).

[6] Similarly, widespread use of services like Content Delivery Networks (CDNs) and reverse proxies does far more to make the Internet secure and reliable than facilitate malicious activity.

Cloudflare strongly believes that extending KYBC provisions would significantly exceed the original scope and carefully balanced objectives of the DSA, introducing unnecessary complexity and unintended harm without delivering meaningful benefits.

IV. The need for transparency and basic safeguards

Given the ongoing aggressive enforcement actions in multiple Member States, including actions that have blocked significant amounts of lawful content during the period of football matches, rightsholders should now have significant evidence about the effect of such practices. In particular, rightsholders have calculated the cost of piracy as a loss of legal subscriptions to content. To the extent that they are seeking additional legislative measures, rightsholders should therefore be required to report on their subscription numbers so the effect of the ongoing initiatives can be properly evaluated.

The single-minded focus on blocking often prompts rightsholders to continue pushing for additional measures, indiscriminately targeting and severing different ways of accessing the Internet. Rightsholders have largely not pursued efforts, referenced in the Recommendation, that might expand the amount of users of their public offers[7], or address fundamental issues regarding their own business models which would lead to users being offered less expensive options.

Given the extensive damage rightsholders' overblocking actions have caused to Internet users and lawful businesses whose content has been blocked, it is reasonable that regulators hold rightsholders accountable. Cloudflare believes regulators' intervention should include the following elements, all of which provide basic safeguards that will help protect the rights of affected users and businesses.

A. Conditions to be met before blocking is even considered

- Blocking should only ever be used as a last resort to reduce local access to pirated content.
- Blocking orders should never extend to core, global Internet technologies such as global DNS resolvers and VPNs.

B. Transparency requirements and due process

- Rightsholders should be required to demonstrate that they have unsuccessfully attempted notice-and-takedown procedures with content hosts or platforms before requesting blocking measures, and should be required to provide notice to relevant intermediaries before pursuing blocking.
- To the extent that blocking is pursued, all blocking requests should be formally justified to and independently verified by a designated government or independent regulatory body.

[7] Commission Recommendation on combating online piracy of sports and other live events, page 7

Such bodies should be required to perform additional checks to assess whether the measures are proportionate and evidence-based.
- A contemporaneous transparency reporting requirement for rightsholders detailing the domains blocked, and when those blocks were implemented, should also be required. A reporting mechanism should track the identity of the requesting parties and associated blocking actions. This data should then be used to measure the effectiveness of blocking requests and resulting collateral damage.

C. Possible remedies associated with blocking

- To the extent that efforts to address piracy result in overblocking, rightsholders should be liable for any economic or reputational harm to non-targeted third parties, with associated penalties/damages. Compensation mechanisms should be clearly defined and enforceable by a dedicated government body.
- Rapid response systems should be public and readily available to any impacted parties, including service providers, to rectify any incorrect or overbroad blocking measure.
- An independent dispute resolution body should be empowered to hear appeals from any of the affected parties. This would ensure that enforcement actions are subject to legal review and procedural fairness.

V. A constructive path forward

Rather than considering additional legislation, we urge the Commission to consider a more constructive approach in tackling piracy online. Effectively dealing with piracy of live events will depend on multiple solutions being deployed simultaneously, combining sharing of data, law enforcement measures, industry cooperation, and measures for distribution of legal content that better satisfy the demand. This challenge should not be left solely in the hands of rightsholders, whose actions have repeatedly demonstrated a narrow, self-interested approach, rather than one that serves the broader public interest. Cloudflare believes that any efforts to combat illegal piracy should be pursued through collaborative efforts that do not impinge on the right of millions of Europeans to browse the Internet:

A. Industry and rightsholder partnerships

- Criminals who make money from illegal streaming activities adapt in real time, shifting tactics and providers to avoid detection and action. The most effective way to address that adaptation is to have strong partnerships between rightsholders and different types of service providers that enable similar shifts in response.
- Cloudflare has pursued a variety of successful partnerships that help rightsholders identify where content is located and enable real time disruption of streaming content.
- Unfortunately, increasingly aggressive and litigious approaches from rightsholders make the type of collaboration proposed in the Recommendation impossible. Rightsholders

should demonstrate a genuine commitment to collaborate with intermediaries before calling for further action.

B. Improve efforts for removal of content

- Mechanisms that enable sharing of information about where content is hosted, best practices related to notice and take down, and identification of domains that regulators have determined to be dedicated to piracy should be encouraged.
- Intergovernmental collaboration is also critical, given most websites that host illegal content operate across borders. Coordinated enforcement mechanisms on bad actors to comply with take down notices, for example, can be crucial when tackling major piracy networks.

Conclusion

The European Commission should resist excessive requests to expand network level blocking as a means to tackle piracy. Given the significant concerns about the way these efforts have been implemented, additional legislative efforts could exacerbate existing challenges.

Existing mechanisms for tackling illegal content already exist through the DSA, and should be allowed the time to come into effect before resorting to disproportionate mechanisms and misguided legislation that could lead to overblocking and undue consequences on the overall functionality of the Internet.

We look forward to discussing these matters further with you.