EuroISPA contribution to the Call for Evidence aimed at assessing the Recommendation on combating online piracy of sports and other live events

ISPs and online piracy

EuroISPA acknowledges and supports the European Commission's efforts to tackle online piracy of sports and other live events, and recognises the complexity of finding effective solutions. However, we are deeply concerned by the approach taken by some European rightsholders and certain Member States, who have implemented disproportionate network blocking measures. Such actions risk undermining the goal of addressing unauthorised retransmissions in a balanced, effective, and proportionate manner.

The illegal dissemination and transmission of live content such as sport events bears challenges for ISPs. Not all service providers are equally able to stop such an infringement in a timely, effective and proportionate manner. ISPs can only reply to an order by an authority by blocking the domain name of the website where the illegal content is hosted, but cannot take down the single problematic piece of content.

When it comes to online piracy, the main ISPs involved are providers of hosting services, internet access providers, content delivery networks, reverse proxies, alternative Domain Network Services resolvers and proxy services. Generally, access providers are the furthest from the actual infringement, as they merely provide the Internet transmission infrastructure which both the rightsholder and the infringer use to disseminate content.

Key issues for EuroISPA

1. The KYBC principle

Demands like expanding the **KYBC (know-your-business-customer)** provision (Art. 30 DSA) could introduce extra risks for the ISPs and might undermine the Internet as a whole. Furthermore, a broadened scope risks reigniting discussions on a matter that was already settled during the DSA legislative process.

In general, additional legislative proposals that would call for inclusion of all intermediaries (including VPN, DNS) must require an accurate and thorough analysis of legal and technical aspects for each category of such intermediaries.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56

2. "Expeditious" action

EuroISPA cautions against the setting up of removal obligations for intermediaries within timeframes that prevent proper examination of disputed content.

In particular, proposals such as to remove content within a 30-minute timeframe would inevitably lead to the over-removal of content, as intermediaries, especially micro, small, and medium smaller enterprises, would not have sufficient time to perform a proper analysis of the content at hand in order to determine its (il)legality. In order to avoid liability and potentially high fines, intermediaries would be encouraged to rather remove content when in doubt, risking the removal of content that has been legally provided by one of their customers. As such, it would put hosting providers in legal risk either vis-à-vis their customers, in case they remove actually legal content, or vis-à-vis the notifier, in case the content is not removed.

3. Over-blocking

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. Introducing guardrails for dynamic blocking to avoid over-blocking, including a clear rapid channel for reversing errors and over-blockings is essential.

Despite numerous over-blocking incidents, certain Member States continue to escalate their efforts and have therefore taken increasingly aggressive measures to expand blocking orders beyond local ISPs who only serve users in their geographically limited market to service providers outside their jurisdiction that offer Internet infrastructure services globally.

Over the last two years, in particular, network blocking at the national level has led to significant legal and economic challenges and we have observed particularly worrying practices in Austria, Italy and Spain that have led to incidents of over-blocking and collateral damage on innocent parties.

4. The need to maintain a safe and open Internet

Efforts in pursuing network blocking measures to combat online piracy are misguided and undermine the integrity of the open Internet. It is fundamental to maintain a safe and open internet, characterised by proportionate and implementable rules.

Preserving the integrity of the Internet infrastructure is of paramount importance, as any measure imposed on a provider can impact all its users and potentially interfere with their (fundamental) rights. For this reason, EuroISPA believes that collaborative approaches between rightsholders and intermediaries are more effective than relying on court orders and invites rightsholders to engage directly with ISPs rather than pursue legal action against them.

The ultimate goal should be to bring together stakeholders – despite their potentially conflicting business interests – to collaborate on finding practical and sustainable solutions to piracy online.

5. Cost reimbursement

Even when web blocking injunctions are requested by a court or a relevant public authority, in full respect of fundamental rights safeguards, service providers should receive full cost reimbursement by the requesting State. This would be necessary for intermediary services – especially the smaller companies – to offset both the personnel and implementation costs associated with such burdensome requests.

6. DSA Implementation

In general, EuroISPA encourages the Commission to take into account – and give priority to – the DSA implementation timeline in order to avoid overlaps. While there has been progress in the overall setup of the DSA and in addressing online piracy, the November 2025 deadline for assessing the Recommendation is too soon to properly assess the impact of DSA tools on the illegal streaming of live events. The DSA is in fact 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, it should be recognised that both the European Commission and national governments and regulators require time to fully operationalise these obligations.

Furthermore, proposals suggesting that intermediaries such as ISPs or cloud infrastructure 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.

Conclusion

We invite the Commission to take into account all the above-mentioned elements and advocate for a collaborative approach grounded in strong industry-government partnerships and enhanced content removal efforts. Additionally, we encourage rightsholders to continue engaging in this dialogue around the Recommendation on combating online piracy of sports and other live events, including by reflecting on structural aspects of their business models that may inadvertently drive users toward unauthorized alternatives.

Case studies

Italy: The Piracy Shield (introduced by Law n°93 of 2023) grants rightsholders the ability to direct the blocking of websites suspected of hosting pirated content in a 30-minute window, without regulatory supervision or transparency. In February 2024, this resulted in a block on a Cloudflare IP address rendering tens of thousands of websites being made 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, due to erroneous reports from trusted flaggers. In both of these instances innocent Internet users, small businesses and website owners suffered disruption and economic damage from the blocks, with no transparency around either that they were blocked or why

they were blocked, nor any mechanism for redress.

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, Italian authority 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.

After just one and a half years of operation of the Piracy Shield, Italian ISPs are actively blocking access to tens of thousands of specific IP addresses and domain names only on behalf of the football-related events "certified flaggers." AGCOM now intends to expand the role of certified flaggers to include other types of live events beyond sports, putting even more pressure on Italian ISPs.

Spain: In Spain, LaLiga, the country's Premier Football League, and Movistar+, a subsidiary of Telefonica, obtained a blocking order from Barcelona Commercial Court No. 6 that allowed both parties to compel Spanish ISPs to deny access to IP addresses they linked to illegally streaming LaLiga 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. The order inevitably led to millions of Spanish users being blocked from accessing thousands of unrelated websites.

LaLiga secured the blocking order without notifying 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 violates the principle of net neutrality. This was also acknowledged by the **Austrian** regulator which, as a result of an over-blocking incident, outlawed IP address blocking due to its associated risks of over-blocking.

Austria: In August 2022, a rightsholder association requested several Austrian access providers to block access to a list of IP addresses, claiming that they were used by illegal music download websites. When access providers blocked access to these IP addresses, many other legitimate websites were also inaccessible, including online shops, news websites and NGO websites. The reason was that these IP addresses were attributed to the same content delivery network, hence by blocking the IP addresses, the access providers also blocked access to all other websites using this same address.

France: Following the implementation of Law n° 2021-1382 on the regulation and the protection of access to cultural works in the digital age, more than 7000 domain names have been blocked. In November 2024, the French audiovisual and digital communication regulator, ARCOM, pointed out in its report on sports online piracy two new trends: the fall of the use of traditional channels (streaming and live streaming, direct downloading et peer-to-peer) and, in opposite ways, the increasing risk of illicit IPTV services. Between 2023 and 2024, the number of blocking measures against IPTV services have quadrupled.

Belgium: Some providers started implementing dynamic blocking injunctions in the framework of the Copyright Directive. The identification of mirror websites is handled by authorities in Belgium, providing clear guidance and legal certainty for ISPs, thereby enabling them to take prompt and appropriate action. In a recent illegal IPTV case, ISPA Belgium member Orange Belgium implemented DNS blocking of 100 websites simultaneously, without leading to any technical issues on the network. Unfortunately, this is not the case for all EU Member States; for example, in **Italy**, blocking orders are outsourced to private parties, the so-called "certified flaggers" appointed by the national communications authority AGCOM, causing more uncertainty to the internet ecosystem.

About EuroISPA

EuroISPA is recognised as the voice of the European Internet Services Providers industry, representing over 3,300 ISPs across the EU and EFTA countries.

Internet Services Providers (ISPs) are small or large companies that provide Internet access to the users. They connect users to the Internet through various technologies such as fibre optic, cable, DSL, and wireless networks. They come in various shapes and sizes: from an SME to an international corporation, even the smallest of these organisations is crucial for the functioning and stability of the Internet.

ISPs include Internet Access Providers, Web Hosting Providers, Email Service Providers, Cloud Service Providers, Domain Registries and Registrars, Content Delivery Networks, Virtual Private Network Providers, Data Centres, Internet Exchanges and Online Platforms. ISPs also play a role in implementing Internet regulations and policies mandated by regulatory bodies like the European Union.

For example, ISPs make it possible to timely detect and take down illegal content online and are a key partner of law enforcement authorities in promoting a safer Internet.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56