EU Commission DG Connect – Unit I.2

Rue de la Loi 200

1049 Brussels

Belgium

09. February 2023

ISPA AUSTRIA'S CONTRIBUTION TO THE CALL FOR EVIDENCE FOR AN INITIATIVE ON COMABTING ONLINE PIRACY OF LIVE CONTENT (REF. ARES(2023)256368)

ISPA Austria welcomes the opportunity to provide input to the EU Commission's call for evidence for an initiative on combating online piracy of live content. We are a voluntary business representation and act as the voice of over 220 internet service providers from various fields all along the Internet value chain. Moreover, the majority of ISPA members are SMEs, and as such, face novel challenges from any new legal regime. In our role as the voice of the Austrian internet industry we would like to address the following aspects in relation to combating online piracy of live content:

1. The role of access providers in combating online piracy of live content

ISPA Austria acknowledges that the illegal dissemination and transmission of live content such as sport events bears challenges for rightsholders. Nevertheless, we would like to point out that not all of the service providers mentioned in the call for evidence are equally able to stop such an infringement in an effective and proportionate manner. Generally, access providers are the ones who 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. As any measure implemented by an access provider affects all of its users, those must be taken with great caution to avoid interferences with other internet user's rights.

In practice, the most common blocking method used by access providers is DNS-blocking which allows an access provider to block the request of its users to certain domains in their domain name server (DNS) and therewith deny them access to an infringing website. Such blocking methods however only allow the blocking of a single server-host or a whole domain and not a specific URL such as a specific livestream. In the case of the illegal dissemination of live content the access provider would thus only be able to block access to a whole streaming website. Other blocking methods such as IP blocking, which is also mentioned in the call for evidence, bear a much higher risk for blocking additional services than just the infringing website and are therefore not common in most EU Member States. The reason is that by having merely an IP address it is basically impossible to proactively determine whether also other services than the infringing website are accessed via this IP address. IP lookup tools that are commonly used by rightsholders are often unreliable and

not up to date. Besides, an IP address may not only be used for a website but also for other services such as Voice-over-IP services. Whether another IP address is also shared with other services will most likely only become apparent when the IP address has been blocked by the access provider and these services can no longer be accessed. It should be pointed out that also the European Court for Human Rights sees IP blocking highly critical and pointed out that any blocking of a legal website just because such website uses the same IP address as an infringing website lacks a legal basis and is thus an unjustified interference in the website operators right to disseminate information according to Art 10 ECHR.[1]

A recent example from Austria illustrates this risk very well: In August 2022 a rightsholder association has requested several Austrian access providers to block access to a list of IP addresses, claiming that these IP addresses were used by several illegal music download websites. When access providers blocked access to these IP addresses, many other legitimate websites, including online shops, news websites and NGO websites, were also inaccessible. The reason for this massive effect was that these IP addresses were attributed to the content delivery network Cloudflare and by blocking the IP addresses the access providers also blocked access to all other websites using this Cloudflare address.

It follows, that access providers are very often not capable of implementing tailored measures that would only block access to infringing content. Rather there is always the risk of blocking also additional, legal services as well. For that reason, also the EU legislator in recent legal instruments has either included blocking injunctions only as a last resort – such as in Art 9(4)(g) of the Consumer Protection Cooperation Regulation[2] or Recital 33 of the recent proposal of the Commission for a Regulation laying down rules to prevent and combat child sexual abuse.[3] In other cases access providers have been excluded from the scope entirely, such as in the Regulation on preventing the dissemination of terrorist content online.

Finally, ISPA Austria would like to reiterate that while the Court of Justice of the EU has clarified that also access providers may be regarded as 'intermediaries' within the meaning of Article 8(3) of Directive 2001/29 and can thus be obliged to take measures to prevent its users from accessing copyright infringing websites, such measures must always be necessary and proportionate in order to be in compliance with the access provider's right to conduct a business.[4] A key factor when assessing the proportionality of any interference in this right is whether less intrusive measures would be available to achieve the pursued aim, which is to protect the intellectual property right related to the live content.

In this regard, the Commission should take note of several other – less intrusive – measures that would be available to end the illegal dissemination of live content. First, rightsholders may in

[1] European Court of Human Rights, Application no. 10795/14 *Vladimir Kharitonov v. Russia*
[2] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004
[3] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse 2022/0155 (COD)
[4] CJEU Case C-314/12 UPC Telekabel Wien GmbH [2012] ECLI:EU:C:2014:192, Recital 46; Case C-275/06 Promusicae [2008] ECR I-271, Recital 68

particular turn to the hosting provider, which can be the operator of the website where the illegal stream is embedded or the webhosting provider of that website. Whereas the operator of the website can take down the specific stream a webhosting provider may be ordered to take-down the full website containing the relevant stream. Sending and receiving such notices to hosting providers has been streamlined and simplified by Art 14 of the Digital Services Act.

On the other hand, the tools available to rightsholders to independently prevent the illegal dissemination of live content must also be considered. A particular useful tool would be to individually "mark" the streams by injecting unique information to each stream via digital watermarking or dynamic steganography. These techniques one the one hand significantly impede the retransmission of live streams to a new audience other than the intended one and may on the other hand even allow rightsholders who encounter an illegal stream to retrieve the embedded information and identify the user whose stream is retransmitted. Subsequently the rightsholder may request the provider of the original streaming service to block this user from using the service and even claim damages, as in most cases a has also provided payment data for using the service. This would also significantly disincentive the user to commit future infringements.

ISPA Austria therefore urges the Commission to consider the wide variety of measures available to combat online piracy of live content when preparing its recommendation. Blocking orders for access providers should only be issued as a last resort, when no other measures are available, they can be reasonably implemented and when there is no risk that third party rights will be infringed.

2. Dynamic and live blocking injunctions

The call for evidence specifically addresses dynamic and live blocking injunctions as a possible solution for countering online piracy of live content. In addition to what has been highlighted in the previous section, ISPA Austria would like to underline, that such dynamic and live blocking injunctions would even further exacerbate the problems listed above.

Dynamic injunctions put ISPs in a difficult position where they independently have to assess whether additional domains provided by a rightsholder concern the same internet services that is covered by the initial blocking injunction by a court or administrative body. ISPA Austria would like to highlight that according to Regulation 2015/2120, introducing the net neutrality principle ("Net Neutrality Regulation") providers of internet access services are prohibited to interfere with internet traffic, except for very specific cases.[5] Aside from technical and security-based traffic management measures, according to Art 3(3)(a) an access provider may only interfere with user traffic in order to comply with Union or national law or measures giving effect to such legislative acts, especially orders emanating from a court or a relevant public authority. Introducing dynamic injunctions would go against this principle as such leave it to the rightsholder to claim whether any domain provides access to the same internet service that is covered by the initial injunction and thus infringes the

[5] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union Art 3

same intellectual property rights, i.e. the respective live content is indeed made available to the public without a license also on that service. Only in such cases, the blocking measure would be in accordance with the requirements of the Net Neutrality Regulation. A simple notification by a rightsholder on the other hand does not constitute a sufficient basis for traffic management measures.

Unjustified traffic management measures bear a significant financial risk for access providers. On the other hand, any breach of Art 3(3)(a) Net Neutrality Regulation could be sanctioned by substantial fines by the national regulatory authorities. In addition, the access provider could be held liable for contractual damages by its customers and for compensation for (e.g. advertisement) losses by the streaming service to which access has been restricted. This puts the access providers at serious legal risk that appears to be unproportionate, considering its passive involvement in the infringement. Even where rightsholders would legally and financially vouch for that the additional domains notified by them provide access to the same internet services, any form of overblocking would cause a public outcry among the ISP's customers, in particular where such concerns popular sport events. This may lead to a loss of reputation eventually also cause financial losses due to a churn of customers.

ISPA Austria therefore calls for any blocking of content to only take place following an injunction issued by a court or a public authority and in relation to a specific domain.

Live blocking injunctions on the other hand, in order to be effective, would require very short timeframes of a few hours whereas some rightsholders even demand that websites should be blocked within 30 minutes. If access providers have to implement blocking measures in such a short period of time, they would not be able to check whether other services are affected as well. The risk of overblocking would therefore increase significantly. Considering that most sport events take place on weekends and outside of regular office hours, sometimes even late at night, for example in case of US sport events, live blocking injunctions would also require each access provider to have all the relevant personnel available at any time which includes at least a technician that implements the blocking injunction and a person with a legal background or a member of the management who can make the decision whether to block the specified content. A 24/7 availability of this staff would not only pose significant problems for small and medium-sized companies, but also for larger access providers.

Whereas such short timeframes are also already foreseen in Regulation to combat the dissemination of terrorist content ("TCO Regulation")[6] it must be expected that live blocking orders would be issued on a much more frequent level. Whereas under the TCO Regulation a hosting provider must only act where terrorist content is hosted on its own server, in the case of live blocking an access provider would need to get active every time a live sport event is illegally transmitted on *any* website. The comparison drawn amongst others also by EUIPO is thus flawed.

Finally, any live blocking system could only be implemented in a (semi-)automated manner which would require significant investments on the side of the access provider to have the necessary

[6] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online

infrastructure available. If – despite all concerns - live orders are planned at EU level, they would have to be accompanied by full reimbursement of costs for implementation and ongoing operations due to their complexity and effort, as was already considered by Advocate General Cruz Villlalón in the UPC Telekabel case.[7]

Considering the strong concerns illustrated above, ISPA Austria requests the Commission to refrain from recommending Member States to make use of dynamic and live blocking injunctions to combat online piracy of live content.

Sincerely,

Mag. Stefan Ebenberger

Secretary General

ISPA – Internet Service Providers Austria

ISPA - Internet Service Providers Austria was founded in 1997 and is a non-profit association which represents the interests of more than 200 members from all sectors around the Internet industry as a voluntary interest group. The aim of the organisation is to act as the voice of Austria's digital economy towards politics and the public and facilitate communication within the industry.

[7] CJEU Case C-314/12 UPC Telekabel Wien GmbH [2012] ECLI:EU:C:2014:192 Opinion of Mr Advocate General Cruz Villalón delivered on 26 November 2013 Recital 106

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675