The Motion Picture Association (MPA) serves as the global voice and advocate of the international film, television, and streaming industry. Our members are Netflix, Paramount Pictures Corporation, Prime Video & Amazon MGM Studios, Sony Pictures Entertainment Inc, Universal City Studios LLC, Walt Disney Studios Motion Pictures and Warner Bros. Discovery.

MPA member companies produce and internationally distribute a rich and diverse selection of film and television content, including entertainment, news, children's programming and sports coverage, that is enjoyed daily by millions of Europeans, through traditional linear television channels, on-demand services and theatrical release.

MPA also plays a leading role when it comes to tackling the illegal dissemination of copyright-protected content that harms the thriving digital ecosystem. MPA's goal is to reduce/mitigate piracy through effective enforcement strategies targeting the operators of illegal sites and services, as well as the intermediaries that enable them.

The MPA therefore welcomes this opportunity to respond to the European Commission's call for evidence on Combating online piracy of sports and other live events – assessment of the May 2023 Commission Recommendation. The MPA welcomed the Recommendation on Combating online piracy of sports and other live events as piracy remains a serious problem in the EU. When it comes to tackling copyright infringement, a swift response is crucial in limiting the dissemination of infringing content and the economic damage caused by piracy. In the case of certain types of content, such as live content – when the economic value is almost entirely exhausted at the end of the live broadcast, real-time enforcement mechanisms, including dynamic siteblocking and fast-track legal procedures, are essential.

As recognised by the Recommendation, the current EU framework grants rightsholders powerful tools, including dynamic injunctions. Focus should be placed on ensuring their effective implementation across all EU Member States. When doing so, it is key to ensure that swift action is taken to limit the dissemination and economic damage of infringing content, including through automated and effective siteblocking mechanisms that can be updated in real time, and that internet service providers (ISPs) and other intermediaries, such as search engines and reverse proxy providers, closely collaborate with rightsholders. The MPA considers that the Recommendation is consistent with EU legislation, including the Copyright and Information Society Directive (Directive 2001/29/EC- InfoSoc), the Directive on the enforcement of intellectual property rights (Directive 2004/48/EC - IPRED) and the Digital Services Act.

When the Commission assesses the effectiveness of the Recommendation, we urge you to consider the need for accurate and timely information on the identity of infringers (broad and effective Right of Information claims and KYBC obligations for intermediaries) and the need for effective staydown obligations. While the DSA introduced some helpful provisions to tackle illegal content, including KYBC for marketplaces, it fell short when it comes to tackling structurally infringing operators.

Piracy of copyright protected content remains a serious problem in Europe

Piracy of copyright-protected content, including the unauthorised retransmission of sports and other live events, remains a serious problem in Europe, with over 185.6B visits to movie and TV piracy sites globally in 2023 and 18.9B downloads globally of pirated wide release movies, primetime TV and video-on-demand

(VOD) content. 17.1 million Europeans use illicit IPTV services, or 4.5% of the EU27 + UK population. This share is even higher – 11.8% - among the population aged 16-24.[1]

This growing crisis threatens both the online safety of viewers[2] and, the underlying economics of the creative and cultural industries, thus hampering the growth and sustainability of legal offers.

Piracy must continue to be addressed to ensure that the market functions properly and that "what is illegal offline is illegal online".

Effective and flexible injunctions should be available

The current EU legislative framework grants rightsholders powerful tools to protect their works. As recognised by the Recommendation, these include the ability to seek siteblocking orders, including dynamic orders, on the basis of Article 8(3) of Directive 2001/29/EC (InfoSoc) and Articles 9 and 11 of Directive 2004/48/EC (IPRED). These provisions allow rightsholders to request no-fault injunctive relief, i.e., authorise courts or administrative authorities to issue orders for ISPs and other online intermediaries to disable access to internet services dedicated to piracy. Dynamic injunctive relief is an effective, proportionate and efficient tool in addressing copyright infringement in the ever-changing digital landscape.

Despite the Commission's Recommendation, Europe is missing effective and appropriate implementation of these provisions across all Member States. Germany has not correctly implemented Article 8(3) InfoSoc nor Article 11 IPRED, whereas Poland and Bulgaria have not implemented these provisions at all. Such vast discrepancies inhibit the ability of rightsholders to effectively protect their content.

Specifically in Germany, the "extended" application of the subsidiarity principle according to which rightsholders must first take action to obtain information on the infringing operator, from any hosting provider based in the EU (or in a comparable jurisdiction), if necessary, by suing this EU hosting provider, contradicts the spirit and the aim of Article 8(3) InfoSoc Directive/ 11 IPRED. It constitutes a barrier for rightsholders to obtaining an injunction, undermining the effectiveness of the relief, and directly contradicting the standards set out in Article 3 of IPRED, including that the procedures should not be unnecessarily complicated or costly.

Another issue in Germany is that rightsholders have no access to fast-track procedures in case the infringing service has been operating online for over one month, regardless of whether it has recently uploaded infringing content.

Swift action is needed to limit the dissemination and damage of copyright infringement.

[1] Source: OpSec Security GDPI

[2] Viewers are often the victims of malware leading to identity theft and fraud while using audiovisual piracy sites, apps, Illegal Streaming Devices and Set-Top Boxes. There is on average a 57% chance of an audiovisual piracy app being installed with embedded malware, according to Audiovisual piracy Cyber risk for European consumers – _The rise of malware, (2022).

When it comes to tackling copyright infringement a swift response plays a key role in limiting the breadth of the dissemination and the economic damage caused. Rightsholders need access to quick relief (e.g., fast-track procedures on the merits, preliminary or temporary proceedings).

In the case of live content, the economic value is almost entirely exhausted at the end of the live broadcast. Other content is time-sensitive, for example because of the stage of release through different distribution channels to final audiences. As a consequence, for these types of content, a significant degree of value is eroded in a very short time frame. The unauthorised dissemination of such content during that particular time frame therefore causes additional and significant damage to a wide range of rightsholders and ultimately to consumers as well as society as whole.

MPA is therefore supportive of automated effective siteblocking mechanisms that can be updated in real-time with appropriate safeguards to address emerging infringing streams. In Italy, Greece, Portugal and Brazil automated dynamic systems are available to rightsholders allowing effective real-time blocks.

Moreover, developing dynamic IP/DNS blocking measures via automated platforms is fully in line with EU law, including InfoSoc, IPRED, DSA (Art. 9) and with the EU Recommendation on combating online piracy of sports and other live events, as well as the more recent Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights.

Best practices in dynamic siteblocking procedures allow for swift updating, preferably directly by the ISPs. Burdensome update procedures render siteblocking significantly less effective in decreasing piracy traffic, as delays allow pirate services to gain traffic to their new online location. When a pirate service is blocked, pirate infringing operators register and activate a new domain—often with a similar name—allowing users to regain access, therefore circumventing the initial blocking order. An expeditious updating process tackles not only the operator's circumvention techniques but also some circumvention by users, who are very quickly informed about the new online location of pirated content, mainly via search and social media channels. Dynamic orders and quick updates also allow parties to unblock in a timely manner, in the cases where the order expires, or when the online location no longer leads to the infringing content.

Collaboration between ISPs and rightsholders is essential

Economic operators, such as online intermediaries, which do not themselves engage in infringing activities, are in many cases best placed to bring infringing activities to an end, as clearly recognised in Recital 59 of IfoSoc. Their involvement is therefore necessary to ensure that rightsholders are able to protect their content swiftly and effectively. In countries allowing siteblocking, and particularly where dynamic siteblocking procedures are in place, rightsholders and ISPs typically have a well-established cooperation, based on a regular exchange of information either directly, or via an update review authority. The MPA has overall observed that blocking orders which meet the legislative and administrative requirements, and their subsequent updates, are implemented by ISPs. However, the time frame for ISP implementation varies vastly, being overall shorter in the jurisdictions with swift dynamic processes in place. Ongoing dialogue between ISPs and rightsholders to address existing challenges and, where possible, implement improvements to the siteblocking process (i.e., format of the information sent to the

ISPs via email, via connecting APIs) is essential. Public authorities have proven to be helpful in creating a platform/forum, where such dialogue can take place, in Denmark, Portugal and Italy.

While ISPs play a key role in executing siteblocking orders, the effectiveness of these measures increasingly depends on the cooperation of a broader range of intermediaries that provide essential services to piracy operators. This includes reverse proxy providers, content delivery networks (CDNs), hosting providers, VPNs and search engines. As specifically noted in the Recommendation, these intermediaries are often well placed to contribute to the enforcement ecosystem. Their cooperation is essential not only to enforce court orders, but also to identify targets, avoid circumvention, and ensure that blocking remains accurate and proportionate.

In particular, reverse proxy services should not shield the identity or infrastructure of infringing sites, but rather cooperate with enforcement requests. Intermediaries such as CDNs also have the technical capability to implement targeted blocking at the infrastructure level, which can be a highly effective complement to traditional siteblocking, especially where operators rely on CDN services to deliver pirated content at scale.

Their engagement tends to be necessary to make targeted and technically feasible siteblocking possible. Failing to involve these actors undermines the effectiveness of dynamic injunctions, as pirates increasingly rely on them to obscure their infrastructure and evade enforcement.

Need for accurate information in a timely manner

An efficient process to retrieve accurate information about the infringer in a timely manner is absolutely crucial so subsequent action can be undertaken, and infringements can be stopped.

Right of Information requests (ROIs) are a tool to identify infringers, not a decision on the merits of an infringement. Therefore, prima facie evidence of copyright infringement should be the rule to allow disclosure requests, even in unilateral/ex-parte proceedings. Good examples of fast-track processes are in place in France and Spain, as well as an out of court ROI process in Germany that helps to unburden courts when dealing with justified requests and expedite the process.

A fundamental issue is the scope of the ROI tool. Unfortunately, the CJEU confirmed in *Constantin*[3] a narrow scope of the information to be disclosed following a ROI request, limited to name and postal address. These details are most often inaccurate, thus failing to ensure an adequate protection of intellectual property. This minimal disclosure should not be the benchmark of the details that can be obtained by rightsholders via right of information requests as it provides impunity for online infringers and fails to meet the goal of Article 8 IPRED which is to identify the infringers.

This narrow interpretation is especially problematic in Germany, as well as in other countries, such as Poland, where ROI actions are uncommon and where CJEU case law is used as guidance.

MPA strongly recommends initiatives to ensure that rightsholders have access in all EU Members States to right of information provisions which are effective, meaning 1) the results of such claims can be obtained

[3] https://curia.europa.eu/juris/liste.jsf?num=C-264/19

on a short term, 2) claims are based on prima facie evidence, 3) the scope of ROI claims is broad and without limitation as long as the requested information allows identification of the infringer and/or the scope of the infringement and harm, 4) the tool is available to all rightsholders and therefore are not overly costly or burdensome to prepare. Further, KYBC polices for all intermediaries used by infringing services should be in place (see below). Obviously, ROI orders obtained in one EU Member State by default need to be enforceable in any other EU Members States (Brussels I Recast Regulation) and in signatories of the Lugano Convention.

DSA – a good first step but doesn't go far enough for tackling structurally infringing services

All intermediary service providers should know their business customers (KYBC)

The Digital Services Act (DSA) has put in place Know Your Business Customer (KYBC) requirements, but the scope of these requirements was limited to online marketplaces. This limited approach is a missed opportunity to address the broad range of illegal content and counterfeit, unsafe, non-compliant and substandard products and services online. All online intermediary service providers should know their business customers.

A business cannot go online without a domain name, without being hosted, or without advertisement or payment services. These intermediary services, having a direct relationship with the business, are therefore best placed to make sure that only businesses that are willing to comply with the law have access to their services. To effectively allow the identification of the source and repeated misuse of their services, intermediaries need to ensure that they obtain accurate and complete customer information.

Article 5 of the e-Commerce Directive already contains an obligation on businesses to identify themselves on their websites. However, the Article lacks teeth (i.e., it is unenforceable) and hence businesses that have the intention of making a profit out of illegal content do not comply with this obligation, and do not suffer any consequences.

KYBC duties seem to be an ideal tool, as they impose minimal burdens on legitimate businesses, all of which are easily identifiable.

Compliance with KYBC obligations would be further simplified thanks to the already existing registers created in the context of the 5th Anti-Money-Laundering Directive (2018/843/EU) of 30 May 2018. As a result, much of the information required for legitimate businesses to comply with the lighter KYBC obligations in the DSA is already publicly accessible, including through: National company registers, European Business Register (EBR) and Ultimate beneficial owners register (UBO register).

The availability of these databases renders KYBC obligations easy to implement with minimal administrative burdens as part of the business sign-up process and subsequent re-verifications on an annual basis. There is a plethora of easy-to-use KYC options available on the market extensively used by businesses (and consumer). KYBC is not difficult to implement, and it does not create significant administrative burdens.

Importantly, just to reiterate, these obligations relate to business customers only, meaning that KYBC produces zero burdens for consumers, while conferring the clear benefit that consumers, other businesses, and public authorities can more readily identify the providers of digital services.

In the 2016 consultation on IPRED rightsholders pointed out that the information they obtain with regards to the names and addresses of infringers is often false.[4] In 2017 the Commission also identified the "limitations presented by the anonymity that counterfeiters or infringers may operate under in the digital environment" as a key issue.[5]

The Commission also recently recognised that “the accuracy and completeness of domain name registration data can also play a central role in the enforcement of IP rights” (Recital 14, Anti-counterfeiting Recommendation).

To contribute towards a safer, more predictable, and trusted online environment for the benefit of EU citizens and legitimate businesses alike, the providers of intermediary services should be obliged to collect and verify information regarding the identity of their business customers and to take action when identification provided proves to be incomplete, inaccurate or fraudulent. The MPA has extensive experience in the use of disclosure tools and the analysis of the accuracy of customer information received by intermediaries. It is only verified data, primarily provided by financial intermediaries (follow the money approach focusing on banks, cryptocurrency exchanges, payment processors) that enables the identification of commercial scale copyright infringers.

Removed content should stay down

To combat piracy in an effective and efficient manner, it is vital to ensure that the stakeholders who are best placed to address illegal content act expeditiously to remove and disable access to notified infringing content and take proactive measures to prevent the reappearance of such illegal content (stay down).

The DSA harmonized the notice and action mechanisms “to provide for the timely, diligent and objective processing of notices”, however it failed to improve the efficiency of notice sending and therefore fails to guarantee effective and swift removal of illegal content and ongoing protection of users. It did not establish a clear obligation to remove or disable access to the notified information expeditiously, nor an obligation to prevent the reappearance of the notified illegal information (staydown).

Conclusion

As noted in the Live Piracy Recommendation (2023) EU law already contains the framework to make siteblocking, including the blocking of live events, possible since 2001. Several Member States have effectively implemented these provisions (IPRED, InfoSoc) either via civil or administrative procedures. However, in some Member States siteblocking isn’t available at all, and in other Member States procedures are too cumbersome. Consistent implementation of existing EU law is essential. KYBC is a key enforcement ask and part of a comprehensive content protection approach. Siteblocking addresses piracy at access

[4] https://statics.teams.cdn.office.net/evergreen-assets/safelinks/1/atp-safelinks.html (see page 19)

[5] https://op.europa.eu/en/publication-detail/-/publication/1e3b2f41-d4ba-11e7-a5b9-01aa75ed71a1/language-en (see page 76)

level and should be complemented by KYBC to enable rightsholders to stop the infringement at the source by shutting down the infringing service altogether. Notice and takedown will remain a challenge until these two elements are in place. What is the incentive for a platform to implement effective takedown/stay-down, when it is able to operate anonymously, and it cannot be blocked in a timely way?