AAPA policy paper

Strengthening the fight against online piracy and the protection of intellectual property rights at the European Union level

November 2020

The Audiovisual Anti-Piracy Alliance (AAPA) represents 31 companies involved in the provision of protected audiovisual services, security technology for protecting such services and the manufacturing of products which facilitate the delivery of these services. Our membership is geographically diverse with companies from Europe, the Middle East, Russia and America, and includes the whole audiovisual value chain, such as rightsholders, platform operators, telecommunication companies, OTT providers, broadcasters and technical service providers. Many of our members are global businesses.

Our aim is to tackle piracy, particularly pertaining to the development, promotion, distribution, application or use of technologies aimed at allowing illegal access to content. Members are facing a concerning growth in volume of unauthorised use of protected audiovisual content. Within AAPA, they coordinate intelligence and action through effective law enforcement, dialogue and interaction.

AAPA members ask for an urgent and strong response from the European Union (EU) to reinforce the fight against illegal content online. More specifically:

I. The Digital Services Act should:

- ✓ Clarify the liability regime of internet intermediaries without questioning EU fundamental principles and case law.
- ✓ Provide for a comprehensive "Know Your Business Customer" obligation.
- ✓ Adopt harmonised "notice and action" procedures, including stay down measures, deterrent actions against repeat infringement and specific policies related to trusted flaggers.
- ✓ Include an obligation for passive platforms/intermediaries, in particular streaming platforms and providers of streaming servers (i.e. hosting providers), to provide a real-time takedown tool.
- ✓ Adopt measures to fight the facilitation of "off-platforms infringement".
- ✓ Confirm the public interest nature of the WHOIS database to access Internet domain registrations.

II. As part of a stronger enforcement of Intellectual Property Rights, further EU interventions will be needed to:

- ✓ Issue dynamic cross-border and catalogue/repertoire-wide injunctions
- ✓ Check the transparency of dedicated anti-piracy tools
- ✓ Ensure a useful right of information against copyright offenders
- ✓ Strengthen the "Follow the Money" approach
- ✓ Have a robust IP Action Plan linked to an industrial strategy as part of the next Audiovisual Action Plan.

ISSUES AT STAKE

1. **Piracy involves severe damaging consequences for the entire audiovisual sector and even beyond**

Intellectual Property (IP) rights are at the core of AAPA members' business models. According to a recent EUIPO report on Online Copyright Infringement in the EU[1], audiovisual remains one of the most impacted sectors for copyright infringements. The report pointed out that the average internet user in the EU accessed pirated content 9.7 times per month in 2018 and that TV copyright infringement represented nearly 60% of the total, followed by film and music piracy.

There are two types of piracy impacting the whole audiovisual sector:

- piracy of audiovisual services: unlawful access to entire channels offerings or to specific channels (e.g. via Internet Protocol Television (IPTV) – see below) directly impacting audience or the number of subscribers for broadcasters;
- piracy of audiovisual content: illicit access to content like sports competitions, films and series (e.g. via live streaming, streaming, direct download, peer-to-peer) which impacts the attractiveness of the legal offer in which legitimate providers significantly invest.

The massive illicit consumption of audiovisual services concerns all types of content, ranging from sport competitions to films and TV series. Piracy generally occurs on premium content for which the consequences are even more damaging because it undermines the high value and the exclusivity of their distribution. The functioning of the whole industry is impacted, leading to a **considerable loss of revenue for the entire audiovisual value chain**, including AAPA members, and prejudicing the sustainability of the creative ecosystem and, ultimately, cultural diversity.

There are also various ways in which IP infringements financially support the emergence of other types of crime. The latest joint report by EUROPOL and EUIPO presents examples revealing the direct connection between IP crime and a wide range of other forms of organised criminality, including money laundering, document fraud, cybercrime, fraud, drug production, trafficking and terrorism[2].

2. **The example of an increasingly sophisticated criminal technology: Internet Protocol Television (IPTV) piracy**

Among all these practices, one distinguishes itself from the others due to its steady proliferation: IPTV piracy.

IPTV is a technology that allows live and on-demand streaming of television content online. It has led to a shift amongst broadcasters from traditional modes of broadcasting by air, satellite and cable towards internet-based streaming. While it offers advantages to customers as broadcasters & TV platforms are able to offer flexible online access and video on demand, criminals have taken advantage of the expanding market and the increasing number of subscribers to set up illegal IPTV

[1] *Online Copyright Infringement in the European Union - Music, Films and TV (2017-2018), Trends and Drivers*, EUIPO - European Union Intellectual Property Office, November 2019, https://euipo.europa.eu/ohimportal/en/web/observatory/online-copyright-infringement-in-eu.

[2] *IP crime and its link to other serious crimes - Focus on Poly-Criminality*, EUROPOL and EUIPO joint case book, June 2020, https://www.europol.europa.eu/publications-documents/ip-crime-and-its-link-to-other-serious-crimes-focus-poly-criminality

platforms. Both the barriers for criminals to enter this market and the corresponding penalties are low, while the rewards are high. In other words, IPTV piracy is a low risk, high return business.

IPTV piracy represents now the most rapidly expanding means of illegal access. Criminals make it possible to watch audiovisual content online through a TV-connected Android box which allows users to access thousands of pay channels by purchasing an illegal subscription at a very low price. In the past, pirated contents were available only in poor quality on insecure websites and/or required downloading risky files from peer-to-peer. IPTV has brought piracy into the home and directly on to the TV as users require minimal technical knowledge to set it up. Using familiar social messaging platforms like WhatsApp, Viber or Discord to operate customer services, communication apps are ensuring frictionless access to pirate services.

An EUIPO study recently estimated that 941.7 million EUR of unlawful revenue was generated by copyright infringing IPTV providers in the EU in 2018 and that these services were used by 13.7 million people in the EU (3.6% of the EU-28 population)[3].

3. A phenomenon which dramatically accelerated during the pandemic outbreak

While millions of people were (and still are, to some extent) locked down at home, looking for different types of digital entertainment to cope with social isolation, criminals have exploited the crisis and adapted their operations to expand their illegal activities.

EUROPOL recently shared concerns about the capacity of criminals to adapt their pirate IPTV offers to global lockdown measures during the Covid-19 outbreak. Pirate offers have increased in number and quality, taking advantage of the lack of sport events and the reduction in the stream quality being delivered by legitimate providers due to EU broadband overload[4].

More generally, according to data sourced from MUSO, a London-based company that provides statistics on piracy activity, **the illegal consumption of films and TV programmes has significantly increased by over 33%** since lockdown measures were enforced worldwide in March 2020[5].

Furthermore, a loss of quality and a declining response rate from online intermediaries to notices during the crisis has been observed. Fighting against piracy should not be affected by any external factors like remote working conditions. Adequate means should be provided to make sure online platforms[6] adapt to all situations, especially in times of crisis, in order to maintain a sufficient level of involvement and responsiveness. The challenge is to develop and ensure the implementation of tools that are sufficiently secure for use in both remote working situations and at the workplace.

---

[3] *Illegal IPTV in the European Union - Research on Online Business Models infringing Intellectual Property Rights - Phase 3*, EUIPO - European Union Intellectual Property Office, November 2019, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf

[4] *Covid-19: Illegal Streaming*, dedicated page on EUROPOL website, https://www.europol.europa.eu/covid-19/covid-19-illegal-streaming

[5] *Film & TV Piracy Surge During Covid-19 Lockdown*, dedicated page on MUSO website, https://www.muso.com/magazine/film-tv-piracy-surge-during-covid-19-lockdown

[6] The term "online platform" encompasses several categories: UGC platforms, social networks, search engines, online marketplaces, and hosting providers.

OUR CALL TO THE EU INSTITUTIONS

Against this background of fast-evolving and ever-increasing sophistication of piracy means, **an urgent and strong response from European decision makers is needed to reinforce the fight against illegal content online**.

The European Commission's intention to lay down "more stringent" rules for the responsibilities of digital services with the forthcoming Digital Services Act (DSA) is encouraging. We call on the EU institutions to provide effective tools to enforce IP rights, through the DSA and other enforcement instruments. All initiatives should focus on enabling the audiovisual industry to keep investing in creative content while at the same time preserving European cultural diversity. This means that these initiatives should in no event lead to new or broader liability privileges, exemptions or protection regimes for digital services that already exist in EU law, which would be inconsistent with the objective of effectively addressing illegal content.

Because our members' contents are usually finger-printed and/or watermarked, illegal transmissions are easily and swiftly identified without any room for interpretation. Consequently, the regulatory enhancements proposed below should be dealt with separately from any regulatory response to issues of harmful content (whether illegal or legal) online.

HOW CAN THE EU INSTITUTIONS HELP, CONCRETELY?

1. **The Digital Services Act is of key importance to:**

- ✓ **Clarify the liability regime of internet intermediaries without questioning EU fundamental principles and case law**

  The DSA offers the possibility of consolidating the European acquis, in particular the e-Commerce Directive[7] and the case law of the Court of Justice of the EU interpreting this instrument, as well as introducing new obligations that would review the existing framework, which is not satisfactory for live content. In particular, the notion of "expeditious" removal should be revisited. This will favour better and safer use of the Internet, while providing legal certainty to all stakeholders.

  A proper "duty of care" should apply to the so-called "passive platforms", without putting into question current exemptions applicable to online intermediaries in the e-commerce Directive.

  The fundamental distinction between "active" and "passive" services must be upheld in the DSA. According to Recital 42 of the e-Commerce Directive, and as confirmed by the CJEU case law[8], only so-called passive intermediaries can benefit from the limited liability regime ("safe harbour") for hosting providers. Where a service provider engages in the processing of user data and/or user (generated/uploaded) content; exercises editorial functions/judgment; commercialises, optimises, and/or promotes that content, including by means of automation, it plays an active role of such a kind as to give it knowledge of, or control over, the content such that it should not be able to rely on the liability exemption. Automation is commonplace

[7] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.)
[8] CJEU Google France C-236/08 à C-238/08 and CJEU L'Oréal SA ea /eBay, C-324/09.

among new digital services and it is a business strategy of providers to automate certain functions. Automation enables these services to engage with user-generated content, by optimising its presentation and recommending or promoting it to a wider audience in order to attract more views and to commercialise it (e.g. by generating and maximizing revenues derived from advertising placed alongside content). AAPA believes that it would be contrary to the objectives of the DSA in terms of tackling illegal content if such services, whilst extracting significant (financial) value from content, were able to benefit from the safe harbour as a passive intermediary.

Yet, certain digital services are trying to challenge the distinction between "active" and "passive" services by wrongly arguing that taking proactive measures on a voluntary basis would lead to a loss of the benefit of the safe harbour principle. It is, however, indisputable that the loss of a liability privilege arises more from the promotion of illegal content for commercial purposes and not from having taken down/disabled access to illegal content. Those who challenge the "active" and "passive" distinction ask for the transposition of the US Good Samaritan principle, yet much criticized there, to the EU legislation. AAPA members strongly oppose such a principle which, in reality, is an attempt to introduce a new liability exemption. The EU Courts have underlined (based on existing provisions) that online intermediaries whose services include categorisation, indexing, search functionality and tagging are not covered by the safe harbour principle.

- ✓ **Provide for a comprehensive "Know Your Business Customer" obligation**

The AAPA welcomes the European Parliament's Internal Market committee report that favours a "Know Your Business Customer" (KYBC) principle. This obligation should apply to all digital services, irrespective of their active or passive nature, making it mandatory to collect the data and verify the identity of business customers wishing to use their services (via the use of company registers or the submission of administrative documents). This verification must take place at the beginning of the commercial relationship and be checked on a regular basis. Such an approach is comparable to procedures already in place in other sectors, such as the financial sector under EU anti money laundering legislation.

The KYBC obligation would also complement Article 5 of the e-Commerce Directive, which imposes a general information obligation on service providers, but which is not enforced enough and does not prevent the distribution of various forms of illegal content online.

Therefore, interested parties should have a means to request digital services to disclose information about their business customers. If a business customer is not identifiable or has provided false information about their identity, the digital service should terminate the business relationship with that customer and cease providing its services.

Financial penalties for non-compliance should be established to ensure that the KYBC obligation is properly implemented.

- ✓ **Adopt harmonised "notice and action" procedures, including stay down measures, deterrent actions against repeat infringement and specific policies related to trusted flaggers**

These procedures would only apply to intermediaries which meet the required conditions to benefit from the limited liability regime foreseen by the e-Commerce Directive.

These notice and action procedures would include:

- **Harmonize take down notices** with (i) standardized broader criteria to justify take down requests, (ii) the possibility to notify several links in one request (very often it is only possible to notify one link/URL, unjustifiably delaying the removal of illicit content) and (iii) in the absence of a notice and take down form an obligation to fill out clear contact information where the request can be sent.
- An obligation to implement an **expeditious removal for live content**: the removal should be immediate when the notification has been received, or at least take no more than 30 minutes[9]. Procedures for appeals against take down notifications should not result in the removal of illegal or potentially illegal content being delayed.
- An **obligation of suspension** in the event of the reappearance of a content previously taken down ("stay down");
- A clear written anti-piracy policy with **deterrent measures against repeat infringement** (for example by restricting, or even blocking, access to users who have been reported multiple times for downloading / uploading illegal content on platforms);
- Platforms should be required to implement **additional layers of verification to user accounts** in order to prevent pirate services from creating multiple accounts that can be used to upload illegal content and bypass any suspension or blocking. Indeed, technological developments have made it possible to create a user fingerprint to prevent that user from circumventing a blocking by creating multiple accounts.
- **Specific policies listing trusted flaggers**, defining their role and enabling fast intervention.

✓ **Include an obligation for passive platforms/intermediaries, in particular streaming platforms and providers of streaming servers (i.e. hosting providers), to provide a real-time takedown tool**

This is the most effective and proportionate way to achieve expeditious notice and stay down. It is neither especially costly, nor complicated for intermediaries to implement. Where such tools have been made available, they have had a very positive and significant impact on piracy.

✓ **Adopt measures to fight the facilitation of "off-platforms infringement"**

One of the big issues with the major online content sharing platforms (e.g. YouTube or Facebook) currently is not just the illegal content stored on their platform, but material posted on their platform that directs users to other places which supply illegal content (e.g. by listening to tutorial video and/or by following hyperlinks in the videos, or in the comments, to streaming websites).

[9] As requested by a Court in The Hague, Netherlands, in a judgment of January 24, 2018, in a case opposing the Football Association Premier League against Ecatel (C/09/485400 / HA ZA 15-367)

As long as the illicit content is not stored on the online platform, the Copyright Directive cannot apply. Today, indirect access to illicit contents via hyperlinks shared on online content-sharing platforms prevails over the consumption of video stored on such platforms.

Online content sharing platforms do not tend to see indirect access to illicit content as their problem, while this is highly damaging for rightsholders. Measures should be taken at EU level to increase liability and duty of care of online content sharing platforms in this respect, regardless of whether such online content sharing platforms are considered as active or passive hosting service providers.

✓ **Confirm the public interest nature of the WHOIS database to access Internet domain registrations**

With the entry into force of the GDPR, access to WHOIS data, which are essential for combating illegal content online, has been restricted through the introduction of a temporary policy specifying under what conditions registrars and registries could collect and process the vast majority of WHOIS data relating to European domain name holders. It was also requested that the entities, which made the request, prove that they pursue a "legitimate objective". This has resulted in the removal of a large amount of data from the public WHOIS registry, impacting the ability of consumers, rightsholders, government agencies and other interested parties to obtain the data necessary to ascertain the origin of goods and services that they wish to purchase or seek redress on, through coercive measures.

2. More generally, as part of a stronger enforcement of IP rights, further EU interventions will be needed to:

✓ **Issue dynamic cross-border and catalogue/repertoire-wide injunctions**

Meaningful enforcement measures include the creation of injunctions as they represent a key remedy for rightsholders against all types of digital services to tackle IP rights infringements. These injunctive reliefs must be:

- dynamic, flexible and expeditious enough to remain effective over time, irrespective of the online locations which can evolve easily (i.e. URL addresses);
- cross-border to avoid lengthy and costly legal actions on a country-per-country basis;
- repertoire-wide to cover the entire rightsholders' catalogue.

In addition, a central repository/database could be set up for site blocking injunctions issued by member states at the EUIPO. The latter could verify the details of the injunctions and provide translations into all official EU languages. This site-blocking record could then be used as a reference by rightsholders to have ISPs implement the blocking in their local territories.

- ✓ **Check the transparency of dedicated anti-piracy tools**

  Greater transparency is needed regarding all types of tools dedicated to anti-piracy such as Artificial Intelligence (AI) tools. More generally, content recognition tools deployed by online platforms to detect illegally uploaded copyright content should be made transparent to an independent authority (at national or European level) and regularly audited to make sure they do not include pro-piracy bias and that they cover the full spectrum of uploaded content with the same conditions. The Commission's guidelines on Article 17 of the Copyright Directive could address this issue.

- ✓ **Ensure a useful right of information against copyright offenders**

  In the recent *Constantin* decision[10], the CJEU regrettably held that content sharing platforms are only required to provide copyright infringers' physical address and not digital information such as their IP or email addresses. Rightsholders should however be guaranteed an optimal information right against copyright infringers by virtue of Article 8 of the Intellectual Property Rights Enforcement Directive (IPRED)[11].

- ✓ **Strengthen the "Follow the Money" approach**

  In addition to binding legal actions, strengthening the so-called "Follow the Money" approach (i.e. seeking to deprive commercial-scale IP infringements of the revenue flows that make their activities profitable) on a European scale would be a complementary solution to tackle the business of piracy involving all stakeholders.

  For example, the Memorandum of understanding (MoU) on online advertising and IPR, initiated by the European Commission to limit advertising on websites and mobile applications that infringe copyright, showed some encouraging results at national level, when Member States adopted a similar approach.

  Going beyond this MoU by setting a European black list of illegal websites, including established outside the EU, which would be regularly updated and sent to all intermediaries involved in the online advertising sector, would be a good way to fight against the placement of ads on websites dedicated to illegal content.

- ✓ **Have a robust IP Action Plan linked to an industrial strategy as part of the next Audiovisual Action Plan**

  More generally, EU decision makers must adopt a holistic and coherent approach when tackling illegal content and supporting the creative sector, especially in the context of the forthcoming IP Action Plan, which we call on the European Commission to draw in accordance with a long-term industrial strategy and in line with the Audiovisual Action Plan.

[10] Constantin Film Verleih GmbH v YouTube LLC & Google Inc (C-246/19)

[11] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.