



AAPA's Contribution to the European Commission's Public Consultation on the Counterfeit and Piracy Watch List for 2022

The [Audiovisual Anti-Piracy Alliance \(AAPA\)](#) welcomes DG TRADE's initiative to update its "Counterfeit and Piracy Watch List". This opportunity is key to highlight the main actors involved in intellectual property rights (IPR) infringement outside the European Union (EU), and raise consumer awareness about these.

For the [members of our Alliance](#), this consultation also offers an opportunity to underline the harms caused by piracy against the whole European audiovisual value chain. The challenge of audiovisual piracy needs to be met on multiple levels, including educational campaigns, use of technology, and increased enforcement activity. However, this needs to be led by action from legislators and policymakers across a range of instruments to create a fit for purpose regime and allow effective enforcement.

This contribution should be seen by the European Commission as a complement to, rather than an aggregation of, our members' individual contributions to this consultation.

About AAPA

The Audiovisual Anti-Piracy Alliance ([AAPA](#)) represents 29 companies involved in the provision of protected audiovisual services, security technology for protecting such services, and the manufacturing of products that facilitate the delivery of these services. Our membership is geographically diverse, with companies from Europe, the Middle East, Russia, and America. It 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 regarding the development, promotion, distribution, application, or use of technologies to allow illegal access to content. Members face a concerning growth in the volume of unauthorised use of protected audiovisual content. AAPA, coordinates intelligence and action through effective dialogue and interaction with other stakeholders and law enforcement.

AAPA's Piracy Watch List

The below provides a non-exhaustive list of operators and service providers identified by AAPA members as problematic with regard to piracy of audiovisual content. This contribution aims at completing the previous Counterfeit and Piracy Watch List, published by the European Commission in 2020. Only operators which were not already part of this list will appear below. When possible, we have mentioned the country/region of the establishment of the companies allegedly or effectively behind these operators. The operators listed only represent a small sample of a much larger problem which is difficult to quantify.

As mentioned above, this contribution should be seen as a complement to the individual contributions provided by our members, not as an aggregation of these contributions.



A. Cyberlockers

A cyberlocker is an online data hosting service that provides file-storing and file-sharing services for various types of media files and data within a secure storage architecture. They can be accessed globally over the Internet and allow users to easily upload files anonymously from personal devices (e.g., computers, tablets, or smartphones) to a remote hosting server. After the uploading, the cyberlocker usually generates a URL link (sometimes more than one) for the uploaded file. The URL link(s) can then be shared with other users by different means.

While cyberlockers can be used legally, nowadays, we often found illegal content hosted on them. Cyberlockers give access to a substantial amount of copyright-protected content, uploaded anonymously into their hosting servers. Some cyberlockers are willing to cooperate and even have set up Advanced Takedown Tool (ATTs) to facilitate the notice and takedown process. However, this does not represent a norm. Indeed, compliance rates and response times vary heavily (several days is not unusual) and removed content can often easily be re-uploaded.

Top infringers of content :

- Uptostream (Dubai)¹
- Chomikuj.pl (Belize)
- Turbobit.net
- Nitroflare.com
- Fembed.com
- Zippyshare.com
- Gounlimited.to
- Uqload.cil
- Waaw.tv (Russia)
- Upstream.to
- Playhydrax.com
- Mega (New Zealand)
- MediaFire (USA)
- InCloudDrive (USA)
- Netu.tv
- Doodstream.co
- Mixdrop.co
- Streamtape.com
- Rapidgator.net
- Maxstream.video
- 123moviesplayer.com
- Turbovid.me
- Deltabit.co
- Uploadgig.com
- Vidcloud.co
- Dood.watch
- Gomo.to
- Playerhost.net
- Dropapk.com
- Userscloud.com
- Ddl.to
- Uptobox.com
- Ninjastream.to
- Katfile.com
- Fastclick.to

¹ Based on information provided on uptobox.com and uptostream.com "About us" pages, these two websites are published by the following company: Genius Servers Tech FZE - Headquarters Dubai Silicon Oasis, Dubai, UAE.



- Videovard.sx
- Vupload.com
- Streamplay.to

B. Hosting Providers

Hosting provider companies offer the necessary technical means to host many pirate organisation websites and streaming platforms. . . They can offer mutual hosting services (typically for linking/indexing websites), dedicated servers, or CDN services (streaming platforms and IPTV services).

Hosting providers are a notable issue for live streaming piracy (see next section). One of the main problems rightsholders face is that several illegal streaming sites are hosted on the servers of those companies. Some even actively advertise their servers for pirate purposes. Moreover, many non-European companies hosting servers of illegal streaming sites are interconnected with companies based in the EU where they install their servers and data centres.

Two parallel approaches should be taken to address this issue:

- Preventive actions are needed to avoid IPR infringers hosting illegal content easily on the hosting providers' servers notably in imposing a traceability obligation on EU companies to know their customer and the nature of the traffic they are carrying on their own infrastructure. This would contribute to clean up and secure the online environment.
- A high level of responsiveness from hosting providers is necessary when illicit streams are detected and notified to promptly remove the pirated content. In practice, some hosting providers allow responsive solutions and terminate accounts from repeat infringers, but most simply ignore notices from rightsholders.

Main content infringers:

- Yurtech / Virtual Systems (Ukraine)²
- ABC Consultancy / Squitter (Russia / The Netherlands)
- Host Spicy (India)
- CDN77 / Data camp (UK)
- iHor Hosting (Russia)
- Amarutu / Koddos (Hong Kong / The Netherlands/ Seychelles)
- ICME LIMITED
- Ihor Servers
- Amanah Tech Inc
- IP Volume, Inc (Seychelles)
- eStruxture Data Centers Inc.
- NForce Entertainment B.V.
- Online SAS/Scaleway (Illiad Group)
- NameCheap (United States of America)
- Offshore-servers (Russia)
- BlueAngelHost Pvt. Ltd (Pakistan)
- FNXTEC (Brazil)
- Hostpalace

² The Ukrainian Internet Hosting Provider known as Virtual Systems (vsys.host) is fast emerging as the largest hosting provider for international piracy in the world. Virtual Systems seeks business based in part on the statement that "In Ukraine, local data-related regulations are much more tolerant to copyright infringement & different abusers." Virtual Systems openly promotes on its website the fact that it provides a means to avoid takedown requests for piracy. Virtual Systems is now the provider responsible for hosting a large share of pirated content from AAPA's members on illegal websites.



- Titan internet ltd.
- DDOS Guard (Russia/UK/Belize)
- Ophidian network (Seychelles)
- ISTQSERVERSES (Jordan)
- HWSPL-AS-AP HostPalace Web Solution PVT LTD (Inda)
- HOST9X (Hong Kong)
- COOP (US)
- CLOUDFLARE (US)
- INT-NETWORK (Seychelles)

C. Live Streaming platforms

A significant proportion of piracy that our members (especially rightsholders of live content and broadcasters) are facing is related to illegal streaming. Streaming sites/CDN-like platforms offer pirate streamers free/ad-supported/paid services. Some do not require any form of login/account to access their services. Pirate source streams push the live feed from a computer or encoder to the platform and receive a live stream URL they can publish on any online resource.

There are four main elements required to stream illegal content to consumers:

- First, a streamer needs access to a broadcast signal (for example, from a satellite decoder box being used to receive a licensed service). This signal can then be captured and transformed digitally using different methods, including an HDMI splitter, screen scraping, or a video camera to record a feed.
- Once a streamer has captured a signal, the content will be uploaded to a Streaming Platform, which manages the distribution of the footage.
- Then a Dedicated Streaming Server, hosted by a hosting provider, transmits copies of the digital footage.
- Finally, a user interface (such as a website, an IPTV box, an application or USB stick with pre-loaded software) is needed by the viewer.

Therefore, the streaming server is a crucial link in the distribution chain. Thousands of consumers can access a single server using different websites, apps, IPTV boxes, and other devices. It is also worth noting that hardly any hosts remove infringing content and when they do, it is made available again shortly after. One of the reasons is that hosting providers often have servers in multiple locations which means that a website could be hosted inside or outside of the EU depending on the day. Sites can also jump from one hosting provider to another making their location difficult to identify.

Main content infringers:

- telerium.tv
- assia.tv
- acestream.org
- wstream.to
- livestream.com
- wigistream.to
- ezcdn462.net
- uzcdn828.net
- jokerswidget.com
- cloudstream.to
- stephn.xyz
- wmsxx.com
- assia.org



- streammart.club
- ragnarp.net
- worldwidestream.net
- liveonlivetv.com
- teleriumtv.com

D. Linking / indexing websites aggregates

Linking/indexing websites aggregates offer live stream content in a user-friendly manner. The live content is typically indexed by live events/competitions, but some sites also list TV channels. The live streams can be watched on an external URL/site or an embedded media player. These actors are especially detrimental to rightsholders and broadcasters of our Alliance. Here too, the lack of Know-Your-Customer rules makes it difficult to geo-locate operators that target European citizens.

Main content infringers:

- cricfree.ws
- www.hulksport.com
- www.crichd.sx
- streamwoop.net
- it.rojadirecta.eu
- daddylive.fun
- sportshub.fan (Buffstreams)
- jokerlivestream.net
- mamahd.ws
- redditoccerstreams.tv
- balkandownload.org
- crnaberza.com
- hesgoal.com
- live.jokerswidget.org
- soccerstreams.co
- usagoals.video
- livetotal.tv
- sportp2p.com
- lshunter.net
- 1rowsports.com
- Footballstream.pw
- Mamahd.live
- Thesports4.xyz
- Sport2watch.xyz
- Cdn.laola1.live
- Sportzonline.to

E. IPTV & Streaming APPs

Internet Protocol Television (also known as "IPTV") is a digital television service delivered through the Internet Protocol network. IPTV is part of a novel service designed to facilitate access to audiovisual content.

IPTV provide access to digital TV over the IP transport medium from a "head-end" device to the final users. IPTV services work on Smart TV's, Android set-top boxes, and applications, but they may also include other services such as web access. The service providers involved in offering **legal** IPTV



services in different countries worldwide are broadcasters, telephone companies, and private network operators, among others.

However, countless illegal IPTV services accessible from most countries worldwide are often sold as low-price subscriptions on different terms (i.e., 1, 3, 6, or 12 months) providing a large number of unauthorized copyright-protected content. IPTV piracy is particularly complex and, in most cases, is related to organised cross-border crime.

More precisely, the website hosting, customer support modules, streaming, and authentication servers of an IPTV service are rarely operated solely from one country. Determining the country an IPTV operator is headquarter in requires an extensive investigation to identify the administrators, and where they are located.

1) IPTV subscription and Service

Closed/subscription-based IPTV services provide users with an online IPTV service for a small fee, offering access to content directly to consumers' without any regulatory oversight that traditional broadcasters are required to comply with. The service can be accessed with a dedicated IP set-top box (STB), or a playlist (m3u8), providing a large number of TV series, movies, and live sports (free/premium). Like legal broadcasters, some services are focused on specific content/markets.

Main content infringers:

- <https://genip.tv/>
- <https://giantiptv.com/>
- King365tv.com (Maghreb area)
- VolkalIPTV.com (Algeria)
- Electrotv-sat.com (Morocco)
- Icone / GogolIPTV (Algeria)
- [iptvitaliaextreme](#)

2) Streaming APPs

Illegal IPTV services are offered via applications downloaded from official stores (GooglePlay and Apple, Samsung SmartTV, etc..). Some of these applications mirror the services offered by IPTV STB's on a subscription model. However, some of the pirate apps make content available for free, and the revenue is gained from advertising within the app. Most of these applications are available globally, providing a large number of international TV series, movies, and live sports channels (free/premium/sports). Still, some services are focused on specific content/markets.

Main content infringers:

- Icone / GogolIPTV (Algeria)
- IPTV Newplay player
- Live Football TV HD Streaming
- All Live Football TV Streaming HD
- Live Football Tv Stream HD (Pakistan)
- Football TV Live App
- Football Live Score TV
- Soccer livestreaming xtra app
- Football360: live soccer app
- Gramface- Live Football Streaming app
- Football Live Score TV
- Live Soccer TV Streaming
- IPTV Newplay player



- Yalla Shoot
- Football Live TV App
- Flix iptv
- Yacine TV Sport
- YASSIN TV
- Yacin Lynx Ip tv
- 020شاهد المباريات مجاناً 2
- IPTV Extreme³
- IPTV³
- IPTV Smartes Pro³
- Ottplayer³
- IPTV Pro³
- OTT Navigator IPTV³

3) IPTV playlist forums

IPTV playlist forums are online forum sites dedicated (or hosting a dedicated group/sub-forum) to the sharing of free IPTV playlists. Forums are organized by the type of content or TV group. This is one of the easiest ways to access live HD content online. However, playlists are usually valid for a short duration of time. The forum sites need to be checked regularly to stay up to date with the latest playlists.

Main content infringers:

- lptvcat.com
- iptvurls.com
- iptv4sat.com
- diavoletto-tv.com
- fr.m3uipvtv.com
- iptvsat.com
- <https://buyyouriptvnow.com/>
- <https://genip.tv/>
- <https://electrosatpro.com/>
- <https://sekoiptv.com/starting/>
- <https://www.iptvpalace.com/>
- <https://www.best-buyiptv.com/>
- <https://bestiptvdeal.com/>
- <https://www.iptvservergate.com/home/>
- <https://iptvgate.com/>
- <https://secureiptv.com/>
- <https://iptvsupply.com/>
- <http://buy-iptvserver.com/>
- <https://buyiptvpro.com/>
- lptvwire.com
- Worldofiptv.com
- Worldofiptv.live

F. TV OPERATORS

Some of our members also market their offers via local subsidiaries around the world. As an example, in some African countries, several local operators with strong local ties and established reputations

³ Information owned and shared by LaLiga antipiracy department. All the information regarding the player apps has been prepared by the antipiracy department of LaLiga with its own tools. LaLiga is a member of AAPA.



(having signs, brands, etc.) illegally market terrestrial television c by broadcasting copyright-protected channels and programmes without the rightsholders' agreement.

It is notably the case of the following two operators. They have deliberately infringed the local IP laws and third party rights for several years. Many of the channels offered by these illegal operators (especially channels that broadcast attractive content such as African and international movies/TV series and sports channels) have been confirmed to be pirated. The channels are pirated in various ways: stolen from legitimate local distributors, or directly stolen from satellites and/or Internet signals before being illegally redistributed, causing significant damage to the rightsholders.

Despite legal court orders and/or administrative decisions in favour of rightsholders, these operators still broadcast channels, and programmes for which they neither have the rights nor consent from the rightsholders.

- SATELLITE CONNEXION also known as "SATCON" (Gabon)

SATCON is a digital terrestrial television (DTT) operator headquartered in Libreville, Gabon. According to the Kantar TNS Institute's 2019 Africascope report, this sports channel (mainly available through SATCON's TV offers) had an audience share of 0.4% in the second half of 2018. It doubled in the first half of 2019 to 0.8%. Several court orders or administrative decisions have condemned SATCON to suspend the broadcasting of programmes and to pay penalties.

- EXCAF TELECOM (Senegal)

EXCAF TELECOM is a digital terrestrial television (DTT) operator located in Dakar, Senegal. According to a study by Omedia Group⁴ carried out in 2019, the penetration rate of EXCAF TELECOM is 9.3%. After a conviction in 2016, EXCAF TELECOM stopped broadcasting some premium sports channels but kept broadcasting others. Several contractual, civil, criminal, and administrative disputes are still ongoing.

⁴ <http://www.omeia-group.com/page.php?page=qui-sommes-nous?>