Introduction

The creative sector is a European strategic asset, a significant provider of jobs and a driver of economic growth. Its future success is reliant upon strong protection of Intellectual Property rights which, in turn, will boost investment and innovation. Today, rightsowners are forced to invest significant sums in protecting themselves against the theft of their content. Piracy in 2024 is big business. It is organised criminality with negative consequences for society, and real risks to consumers. Not only does it line the pockets of criminals, it represents significant losses in tax revenue for EU Member States. Social networks, search engines and faster broadband speeds are making it easier for consumers to find infringing content. The number of entry points to piracy continues to grow and includes online marketplaces, locker sites, linking sites, Apps, IPTV services, social media and so on.

Given the above, the fight against online piracy can no longer rest in the hands of rights owners alone. Real legislative action is needed from legislators and policy makers across a range of instruments to create a fit for purpose global regime. There are tools in the current EU legislative framework that can help but today's challenges for rights owners revolve around the hugely varied interpretation and the lack of enforcement. For example, many hosting providers make substantial money from piracy, often by not acting rapidly enough, or in many cases at all, in response to notices from rights owners sent under the Digital Services Act. When referring to take down, the vagueness of the term "expeditious" is exploited by a number of hosting providers and social media platforms which fail to act upon notices in a way which offers any assistance to rightsowners. For live rights, delay is as good as complete inaction. In some cases, and again despite their obligation under the DSA, non-EU intermediaries offer their services to recipients located in the EU while making themselves unreachable, offering no legal representative nor an efficient mechanism to remove pirate content from their networks.

As such, we welcome the EU Commission's initiative to update its "Counterfeit and Piracy Watch List" of non-EU operators and we are pleased to provide the following data. Please note however that those named in this response represent only a sample of a much larger population of infringers, who are difficult to identify and geographically place due to the ease with which they can make infringing services available within the Union without providing any meaningful information about their identity. As mentioned above, this is a problem which requires urgent attention by the DSA enforcement teams.

Topics (data for January to June 2024, unless otherwise stated)

1. **Hosting Providers**
    a. **Cloudflare**
2. **Marketplaces**
    a. **Facebook Marketplace**
    b. **Alibaba**
3. **Search Engines**
4. **File Hosting Sites**
    a. **Cyberlockers**
    b. **Live Streaming Sites**

5. **Apps**
6. **Social Media**
    a. **Telegram**

1. Hosting Providers

Below is the list of the most infringing and least compliant hosting providers based outside the European Union. These organisations provide dedicated hosting facilities to operators of pirate servers and typically fail to expeditiously remove content, provide information on the infringing operators, or ban those operators from their servers. Some take no action at all. In some instances, the host seemingly encourages questionable behaviour by promoting anonymous registration, offering numerous cryptocurrency payment options, providing offshore hosting and in the case of the Virtual Systems website, outlining their 'lax content policies due to the flexibility of local regulations'.

It is also worth noting that many non-EU based hosting providers used by illegal streaming sites have connections with companies based in the EU, where they install their servers and data centres. Preventive measures including Know-Your-Customer obligations should be imposed on companies that target European users.

Data below refers to the period 1 January 2024 to 29 July 2024

ASN Name	Country	Notes
ISTQSERVERSES, JO [AS211826 & AS212042]	Jordan	• Included in 2022 list of infringing hosts • Remains one of the top infringing hosts • 37,907 unique infringing incidents identified • Upstream of non-compliant hosts AS141718 & AS208949
HHXYTC haoxiangyun, HK [AS141718]	Hong Kong	• 126,242 unique infringing incidents identified
HBING, GB [AS208949]	United Kingdom	• 87,701 unique infringing incidents identified
YURTEH-AS, UA [AS30860]	Ukraine	• Included in 2022 list of infringing hosts • Remains one of the top infringing hosts • 165,871 unique infringing incidents identified

VIRTUAL SYSTEMS, UA [AS6698]	Ukraine	• 110,331 unique infringing incidents identified
RESERVED, ZZ [AS27161	United States	• Top infringing host, formerly known as 'Litnics' • 284,454 unique infringing incidents identified
NETSOLUTIONS, MO [AS47674]	Macao	• 159,580 unique infringing incidents identified
CLOUDFLARENET, US [AS13335] CLOUDFLARESPECTRUM [AS209242]	United States	• Included in 2022 list of infringing hosts • Remains one of the top infringing hosts • 107,307 unique infringing incidents identified

a. Cloudflare

Cloudflare is a Content Delivery Network (CDN) founded in 2009 and headquartered in the U.S. It is now the CDN with the highest number of exchange connections anywhere in the world.

Cloudflare is believed to provide Domain Name System (DNS) services to more than 15 per cent of all known global websites. DNS functions as a reverse proxy server for websites, effectively acting as an intermediary between a visitor to a site and the servers belonging to that site.

The architecture of the service provided by Cloudflare claims to optimise and speed up the distribution of digital resources while ensuring security is maintained. While the services were not created to promote or disseminate infringing content, their characteristics can be easily exploited by pirate operators as they conceal the real hosting provider being used.

Many pirate services are believed to use Cloudflare. This was demonstrated in the 2019 Milan Court Order involving 'EnergyIPTV' and 'IPTVTheBest', with both services using Cloudflare's infrastructure to distribute infringing content, without Cloudflare taking adequate steps to prevent infringement.

The main issues faced by copyright owners trying to protect their content are both technical and legal. Pirate websites using Cloudflare are anonymized, making it impossible to track these sites and pursue them through the courts.

Cloudflare's response to reports, although seemingly compliant with legal requirements, can be unsatisfactory. While Cloudflare will pass on reports of abuse to its customers, it will not assist with identifying the offending hosting provider or interrupt the services it provides. Cloudflare has also refused to comply with Court Orders issued against it by European Courts, for example the Milan Court Order referenced above.

2. Marketplaces

a. Facebook Marketplace

Facebook Marketplace is the most prominently used marketplace by pirates to promote and sell piracy enabling devices (particularly pre-loaded Amazon Firesticks) and IPTV services/subscriptions. Meta states that it has proactive measures in place to identify and remove piracy enabling devices as well as IPTV services from Marketplace, but the continued volume of these listings suggests that the measures are largely ineffective. In the 6-month period between February and July 2024, more than 16.5k listings for modified Firesticks were found and reported on Facebook Marketplace, representing 96% of all modified Firestick listings identified across online platforms in this period.

The relevant policies on Facebook Marketplace need to be updated and improved. While Meta is willing to engage, to date any countermeasures have not resolved the significant challenges faced. Meta should implement significant proactive measures to stop infringing listings being uploaded and/or located by consumers and to ensure that offending traders are not able to create new accounts once any existing accounts have been banned.

b. Alibaba

Alibaba is being used by pirates to openly sell IPTV subscriptions and services targeted at European customers. Sellers are careful not to provide proof of infringement prior to purchase, instead using vague and suggestive terms, such as “all [insert country name] premium channels” or “PPV events”. Alibaba refuse to remove these listings. They should, in accordance with paragraphs (d) (“Any items that can be used to gain unauthorized access to protected, restricted or premium offerings such as television programmes (such as satellite and cable TV), internet websites, telephone applications, information data or other such services, e.g. descramblers and decoders;”) and (j) (“Any other items which may assist an individual in gaining access to unauthorized content, information, control or property;”) in the section 8.1 (“Circumvention devices and other equipment used for illicit purposes”) within Part 2 (“Prohibited Items”) of their Product Listing Policy, act to remove these listings.

3. Search Engines

a. Google

Google Search is the most commonly used search engine, and it plays a significant role in the discovery of infringing content, both through organic search results and so-called sponsored adverts.

While Google will respond to take-down notices against specific infringing URLs, it will not take action against whole domains, meaning that illegal streaming sites can be the subject of numerous individual page takedown requests without any clear delisting impact against the overall site.

Google will not accept delisting requests for pages/sites encouraging copyright infringement, such as sites that openly encourage the use of VPN technology to circumvent pay TV offerings. Google also fails to provide rights holders with functioning APIs for delisting, meaning that the process of submitting delisting requests is manual and time consuming.

Sponsored adverts for infringing IPTV services regularly appear in Google search results, with ads from the same accounts often appearing multiple times, suggesting that repeat infringer policies are ineffective.

4. File Hosting Sites

As a general point, when it comes to file hosting sites (cyberlockers and live streaming sites), the lack of Know-Your-Customer rules makes it difficult to geo-locate operators that target European citizens.

a. Cyberlockers

Cyberlockers are online data hosting services that provide secure file-storing and file-sharing services for different types of media files. Users can access these globally and easily upload files to a remote hosting server. Once uploading is finished, a URL link for the uploaded file is generated by the cyberlocker. This URL link can then be shared by the user in numerous ways, such as a post on a popular linking site, or posts in closed groups on social media platforms and forums.

There are two main revenue models for cyberlockers: paid-for premium accounts allowing access to infringing video content (with an average cost of 10€ per month); or ad funded sites, redirecting users through various URLs before allowing access to content.

Cyberlockers play an important role in anonymously distributing infringing content. Removing this content is a difficult process and users can easily re-upload files that have been removed. Some cyberlockers offer an automatic system for regenerating removed links that can be activated upon payment of a monthly fee. Compliance rates and response times vary widely (several days is not unusual) and some cyberlockers do not even provide any means or contact to report infringements.

The origin of their operation and servers are usually obfuscated, so the information given below can only be used as indication. Determining exact locations is very difficult.

The table of cyberlockers below lists some of the most infringing file hosting sites. In the six months to June 2024, many of these have each been responsible for providing access to tens of thousands of different links to content that infringe copyright.

Cyberlocker	**Notes**	**Piracy Popularity**
Vidcloud.co	• Geolocation not possible (Cloudflare)	#1
Rapidgator.net	• Registration obfuscated • Average response time to notifications more than 72 hours	#2
Chomikuj.pl	• Geolocation not possible (Cloudflare)	#3
Ddl.to	• Geolocation not possible (Cloudflare) • Average response time to notifications more than 72 hours	#4
Mixdrop.co (also mixdrop.sx, mixdrop.to)	• Registration obfuscated • Servers believed to be located in Germany • Subject of High Court injunction in the UK	#5
Dood.watch (possibly connected to dood.so, doodstream.com)	• Geolocation not possible (Cloudflare) • Average response time to notifications more than 72 hours	#6
Nitroflare.com	• Geolocation not possible (Cloudflare)	#7
Streamtape.com	• Believed to be located in Russia • Average response time to notifications more than 48 hours	#8
Voe.sx	• Believed to be registered in St Kitts and Nevis • Servers believed to be located in Belize • Average response time to notifications around 48 hours	#9
Rapidrar.com	• Geolocation not possible (Cloudflare)	#10

b. Live Streaming Sites

A significant proportion of piracy is related to the illegal live streaming of sport. Streaming sites offer free, ad funded or paid services to pirate consumers. Some do not require any form of login/account to access their services. Given the nature of live sport, it is particularly crucial to remove infringing content in a timely manner. Our data shows that levels of compliance among live streaming sites is extremely poor. Even when infringing content is taken down it often becomes available again in a very short space of time.

Sites often have servers in multiple locations or related IPs are concealed (see section 1.a on Cloudflare) and a website could be hosted inside or outside the EU from one week to another. Sites also jump between different hosting providers so the information given below can only be seen as indicative. It is not possible to say with certainty that these sites are permanently based outside of the EU.

Data below refers to the top 10 stream hosting sites for the period 1 February 2024 to 31 July 2024

Hosting site	Total number of incidents	Average uptime (H:M:S)
srv93221.tservone.lol	11,145	01:39:41
iptvtree.net	8,681	13:27:46
myteve.online	7,756	13:18:48
Sansat.net	7,723	13:14:07
myvipmedia.com	7,250	07:31:40
www.sportp2p.com	6,812	11:08:49
azdouiptv.com	6,274	12:36:35
vodkom.net	6,172	12:21:47
tv.pro-ott.com	6,147	15:00:44
aziz.social	6,095	12:31:25

5. Apps

Illegal streaming services are sometimes offered via applications which can be downloaded from official or unofficial stores. Again, there is a mix of paid subscription-based offerings and those offering content for free via an ad-funded model.

The table below shows the list of Free Apps that have been removed from the Google Play Store with an average compliance time between 1 to 15 working days. The list denotes those apps with the highest number of downloads in the 6 months to June 2024, alongside removal time latency.

Apple do not provide equivalent data, and it is extremely difficult to track unofficial app stores. It is difficult to confirm the location of the operators of the apps below, for reasons outlined in the Live Streaming Sites section of our submission.

Developers often use names that include keywords like Live Football TV and Football Live Streaming. This strategy allows them to leverage the popularity of other illegal applications with similar names that have been previously removed from app stores.

Data below refers to apps removed from the Google Play Store for the 6 months to 30 June 2024

App name	Downloads	Response time (days)
RepelisPlus Pelis Stream	10,000+	1
Scarica film | VC	10,000+	14
PTV Sports: Live Cricket TV	10,000+	15
YACINE TV Store	10,000+	5
Football Livestreaming HD TV	10,000+	1
Live Cricket TV 2024	10,000+	1
MovieFlex	5,000+	1
Salama TV – Angalia Mpira Live	1,000+	3
Magis – Peliculas y Series	1,000+	1
Hotlflix	1,000+	1

6. Social Media

a. Telegram

Telegram is a cloud-based mobile and desktop application offering instant messaging services. It can be used to share infringing content for download or streaming and to promote illegal

IPTV services via public ‘channels’. Users can also share links to other sites hosting infringing content or to other marketplaces selling counterfeit goods.

While Telegram may act to remove infringing content, channels discussing or promoting illegal IPTV services remain accessible, often despite being the subject of multiple complaints.

Telegram does not currently have a Content Management System or a video fingerprinting tool to aid in the finding and reporting of infringing content.