IFPI Submission to the EU Counterfeit and Piracy Watchlist Consultation 2026

18 September 2026

IFPI represents the recording industry worldwide, with a membership comprising of some 8,000 record companies in 70 countries and affiliated industry organisations in 70 countries. Our membership includes the major multinational music companies and hundreds of independent record companies, large and small, located throughout the world.

SUMMARY

Music lies at the heart of European culture, and Europe remains a dominant force in the global music landscape. From classical composers who define Western music traditions to modern artists filling arenas, topping charts and building vibrant online communities, European music remains a powerful cultural force. Record labels invest in the wider European music sector, including by developing and promoting new European artists, creating production facilities in their local markets, and by opening new markets in third countries for European artists and European music. They also invest in music companies in third countries. Record labels are the engines of the broader music sector[1] and their ability to continue investing in new talent is dependent on the ability to license their rights on fair economic terms, and to have any unlicensed services closed down, through legal actions where necessary.

Recorded music revenues in the European Union reached EUR 6.0 billion in 2025, growing 5.1 percent year-on-year and accounting for 21.3% percent of global recorded music revenues, according to *'Music in the EU 2026'*, IFPI's annual report examining the performance, impact and future of Europe's music sector. Nine of the world's top 20 recorded music markets are located in the EU, together accounting for EUR 5.1 billion in revenues, while EU recorded music revenues increased by EUR 293 million during 2025.

However, the legitimate music market is still being impacted by online piracy which remains a major concern for the recorded music industry in Europe. Pirated music remains a major barrier to the legitimate trade of recorded music, and it affects the music creators' community in Europe and globally.

In this submission we will address the prevalent forms of music piracy ranging from stream ripping services to cyberlockers, BitTorrent services, and downloading sites. We will also highlight challenges with the enforcement of rights in connection with AI services, as well as the "new form of piracy" – streaming fraud – which has been supercharged by the generation of AI content at scale.

[1] Powering the music ecosystem, IFPI: https://powering-the-music-ecosystem.ifpi.org/

We further raise the serious issue of online platforms including user uploaded content services failing to take effective measures to prevent and stop infringing usage at scale. In that context, we are also flagging the rise of infringing mobile apps and the concerning fact that mobile app stores fail to consistently remove infringing apps despite having been notified of their illegal nature, in line with the requirements of the DSA.

Finally, our submission highlights challenges with intermediaries more generally, such as registrars and registries as well as companies like CloudFlare, which continue to provide a crucial infrastructure to illegal services despite the apparent and ongoing infringements.

What the EU needs to do to address these concerns:

Correct and comprehensive implementation of the current EU aquis: The EU Member States should fully implement the existing EU acquis, including but not limited to IPRED and the DSA. The European Commission should act to ensure that all Member States adhere to the principle in Art. 3 IPRED to provide for effective, proportionate, dissuasive measures (effective injunctive relief, without prohibitive costs, on catalogue-wide basis). That means, for instance that, no-fault injunctions should cover all intermediaries and be awarded as "*dynamic injunctions*", and injunctions covering several Member States should be available in appropriate cases. Further, the Commission should make sure that Member States correctly implement all of the measures and procedures in the DSA and the IPRED including in the context of AI. This should include catalogue-wide remedies based on a reasonable sample of evidence, as foreseen by the Directive.

The EU must ensure meaningful transparency of AI models and an effective single market for enforcement. This could be done by requiring a two-tiered disclosure of the protected works used or data sources accessed for GPAI training and assessing the need to introduce procedural measures to address cases of non-compliance with EU copyright rules and/or the AI Act.

The EU should continue its work on IPR enforcement, including the live piracy recommendation which should also cover time sensitive content. This should include work on notice and action and there should be a clarification that all hosting providers must comply with a notice and stay down regime. In addition, all intermediaries should be obliged to implement effective KYBC procedures, so as to remove the cloak of anonymity from criminal operators.

Law enforcement authorities in EU Member States are often insufficiently resourced to prioritise copyright offences and, in some cases, do not have experience or expertise to handle digital piracy investigations. IFPI is prepared to work with the relevant authorities, in a constructive and transparent manner, to share information and experiences to ensure that illegal services established outside the EU cannot offer their services to EU consumers. IFPI is also prepared to support law enforcement authorities by providing training, expertise and practical guidance in relation to emerging forms of piracy. It is essential that there is effective coordination between units to address poly-criminal activities that impact right holders.

We have set out in the table below a summary of the sites and services we have referenced in our submission.

List of Sites/Services included in our submission
AI
Treblo (previously: Sonauto)
Media.io
Lalals.com
Rythmix: AI Music & Song Maker
MusiQ AI- AI Music generator
Shadow Libraries
Anna's Archive
Mobile Apps
Musi
Youtify
Stream ripping sites
Y2mate.gs (formerly y2mate.nu)
Savefrom.net
Ssyoutube.com
Y2mate.is
YTDL-P
Cyberlockers
Mega.nz/io
Ddownload.com
Pillowcase.su
Turbobit.net
Imgur.gg
Rapidgator.net
Pixeldrain.com
BitTorrent
1337x.to
ThePirateBay.org
MP3 Sites
"Muz" network
Nigerian Blog Sites
Ceenaija.com
Trendybeatz.com
Waploaded.com / Meetdownload.com
Hiphopkit network
Tubidy network of sites
Streaming Fraud
Justanotherpanel.com
Services
X
Discord
Telegram
Vimeo

Intermediaries
Njalla
CloudFlare
Registrars/Registries
Namecheap
Tucows
GoDaddy
Verisign
PIR
Tonic
Physical piracy
Pinduoduo
Shopee

ONLINE SERVICES OFFERING ACCESS TO OR FACILITATING ACCESS TO COPYRIGHT-PROTECTED CONTENT

a) Artificial Intelligence

Generative AI services

There are multiple generative AI services offering music, audiovisual content or generate lyrics. In many cases, IFPI has indication and good reasons to believe that these services have used copyright protected content from our members (sound recordings or music videos) to train their services, often without authorisation.

The outputs produced by these AI models are available via the same distribution channels and can unfairly substitute demand for the very works that are used to train the models, both on licensed music services as well as in the public performance rights sphere. Further, there are valid indications that AI generated music is often used for streaming fraud (see below), e.g. based on the stats recently published by Deezer AI-generated tracks on the platform represent 'more than 50% of total uploads of new music, with a monthly average of 90,000 tracks'.[2] Many of the providers and deployers of the unlicensed generative AI models are established outside the EU, predominantly in the US, China and Singapore, which provides an additional challenge for EU right holders.

Current Litigation Against AI Services

Copyright infringements in connection with AI have become an extremely litigious area both in the EU and beyond. In terms of music cases: in June 2024, record companies filed two copyright infringement cases claiming Suno and Udio, two US-based generative AI services, had engaged in mass infringement of copyright protected sound recordings by copying them

[2] https://newsroom-deezer.com/2026/07/ai-music-exceeds-50-percent-daily-uploads-deezer

for the purpose of training their AI models.[3] While some companies have settled, the lawsuits remain active.

In October 2023, music publishers Universal Music Publishing Group, Concord Music Group, and ABKCO, filed a lawsuit against the AI company Anthropic, alleging direct, contributory, and vicarious copyright infringement as well as copyright management information removal claims. The plaintiffs allege that Anthropic's generative AI chatbot, Claude, generates output that copies the publishers' lyrics when prompted. The case is ongoing, with Anthropic's motion to dismiss being declined.

In 2025, Germany's authors' collecting society, GEMA, successfully sued OpenAI in Germany in respect of unauthorised use of its members' protected song lyrics by OpenAI in the training of ChatGPT. Further, in January 2025, GEMA sued Suno in Germany in respect of alleged unauthorised use of music from GEMA's repertoire to train Suno's AI model. The Munich District Court issued a decision on 31 July 2026 and Suno was found liable for training its model in the US and is responsible for output generated by the model.

There are also a number of cases pending in the EU which have been brought by other right holders with a view to establishing a legal precedent that the training of a generative AI system with sound recordings requires authorisation from the right holders. For example:

- the book publishers have taken action in the US against OpenAI[4] and Meta.[5]
- Getty Images Inc has sued Stability AI, Inc in both the US and the UK.
- RTI and Medusa Film (the broadcaster and movie production company) have sued Perplexity AI in Italy in respect of unlawful use of copyrighted content for AI training.
- SNE, SGDL and SNAC have sued Meta in France in respect of unauthorised use of their members' works to train Meta generative AI models.

Vocal Cloning services

Another group of AI services that causes serious concern to the music industry are the vocal cloning services. Such services enable users to create 'deep fake' tracks where an AI-generated version of an artist's voice is set against a new composition and AI vocal clone covers, i.e. a 'cover' version of a song whereby the instrumental bed from an existing song is combined with a different artist's AI-generated voice. Consumer-facing vocal cloning services in the form of websites, bots and apps have proliferated, allowing users to generate such content without any technical expertise.

The process of vocal cloning typically involves multiple acts of unauthorised reproductions. Further, the outputs will likely infringe both the copyright (or related right) in the original sound recording, and also the personality rights (such as rights in the voice, name, image and likeness) of the individual whose voice has been cloned by the AI model.

[3] Record Companies Bring Landmark Cases for Responsible AI Against Suno and Udio in Boston and New York Federal Courts, Respectively - RIAA
[4] Authors Guild v Open AI Inc
[5] Kadrey v Meta Platforms, Inc

Sonauto/Treblo –

Treblo, f/k/a Sonauto, is an unlicensed generative AI music service based in San Francisco, California. By inputting simple text prompts, users can generate song-length music files in many genres. After the company launched "v3" of its model in early 2026, an analysis by a third-party podcast demonstrated similarities between outputs generated by Treblo's model and pre-existing copyrighted sound recordings. Treblo has not publicly disclosed the contents of its training data.

Based on data from Similarweb, Sonauto/Treblo received over 8 million visits globally in the last 12 months (August 2025 to July 2026). Both Italy and Germany were in the top 10 in terms of traffic to the site in the last 12 months. Treblo also received over 2.2 million visits globally during the same period with France and Italy appearing in the top 10 in terms of traffic to the site.

Media.io

Media.io is an online media-editing platform operated by Wondershare, based in China with offices located globally. The platform has received 54.04 million global visits in the last 12 months (August 2025 to July 2026). The site offers generative AI music models including proprietary models, and AI tools including vocal removal, voice cloning and AI song covers. These features allow users to upload or transform existing recordings and apply synthetic voices, including artist-style voice models, to create new outputs. The service therefore raises copyright and personality-rights concerns where protected recordings or identifiable artist voices are used without authorisation. Media.io should be included on the Watchlist because it provides consumer-facing tools that can facilitate the unauthorised use of music content at scale.

Lalals.com

Lalals.com is an AI-powered audio platform operated by Lalals FZ-LLC, based in the United Arab Emirates. The platform has received 2.509 million global visits in the last 12 months (August 2025 to July 2026). The site offers voice changing, voice cloning, text-to-speech, stem splitting, AI song generation, mastering and AI cover tools. It promotes access to a large library of AI voices, including many popular artists represented by IFPI member companies, and enables users to upload tracks, split stems, generate songs, clone voices and create AI covers, including from source material provided via a YouTube link. These features raise copyright and personality-rights concerns where protected recordings are uploaded, separated or transformed without authorisation, and where synthetic voices are used to imitate identifiable artists. Taken together, the service provides users with a readily accessible means of repurposing protected recordings and creating outputs that may infringe both copyright and artists' voice, image, name and likeness rights.

AI Apps

Rythmix – AI Music and Song Maker

Rythmix is an AI music generation and vocal cloning application available on both Google Play and the Apple App Store. The Android application is published by PROMINENT FORTUNE PTE. LTD., based in Singapore, while the iOS application is published by Vivalive (Hong Kong) Limited. Despite the different publisher names, evidence indicates that the applications form part of the same service: both use the com.song.ailab identifier, share Rythmix branding and associated aisongcreate.com infrastructure, and corporate records identify Prominent Fortune as a subsidiary of Vivalive Hong Kong.

Rythmix provides AI music-generation and AI vocal cloning/cover functionality, enabling users to create music using synthetic voices. As part of its AI cover functionality, testing has identified stream-ripping functionality which allows a user to paste a YouTube URL directly into the application, select an artist voice and use the underlying YouTube recording to generate a new AI cover incorporating the selected cloned voice. This functionality enables copyright-protected sound recordings obtained from YouTube to be used as source material for the creation of AI-generated derivative recordings. The application therefore raises concerns both in relation to the unauthorised acquisition and use of copyright-protected recordings from YouTube and the unauthorised cloning and use of recording artists' voices.

The functionality identified during testing is particularly concerning from the perspective of voice, image, name and likeness (VINL) rights, as users are able to select and apply AI-generated artist voices to existing music without evidence that the relevant artist has authorised the cloning or exploitation of their voice. This combines two areas of concern within a single service: the acquisition and use of copyright-protected source material from YouTube and the subsequent use of AI-generated artist voices to create new recordings.

Why should the app be included on the Watchlist

Rythmix should be included on the Watchlist due to the combination of its stream-ripping functionality and AI vocal cloning capabilities. The ability to provide a YouTube URL as source material substantially reduces the steps required for a user to obtain and repurpose protected music: rather than requiring users to provide independently sourced audio, the application can obtain the source material directly from YouTube before processing it through its AI cover functionality. The resulting service facilitates the creation of recordings combining copyright-protected source material with synthetic representations of artists' voices.

Rythmix is a highly popular application across both major app stores. On Google Play, the app has accumulated more than 5 million total downloads, including 272,577 downloads in the last 30 days, and has reached a highest chart position of No. 4 in the Music category. On the Apple App Store, Rythmix has similarly generated more than 5 million total downloads, including 650,877 downloads in the last 30 days, and has reached a highest chart position of No. 2 in the Music category.

MusiQ AI – AI Music Generator

MusiQ AI is an AI music generation and vocal cloning application currently available on the Apple App Store and operated by Lumetro LLC. The application provides AI song-generation and AI cover functionality, allowing users to generate complete songs and create new versions of existing recordings using different AI-generated voices. Apple's listing expressly promotes its AI Covers functionality and the ability to create and use custom AI voice models, with the application monetised through advertising and paid Premium subscriptions.

Testing of the application has identified functionality similar to Rythmix, combining stream-ripping functionality with AI vocal cloning. Users are able to provide a YouTube URL as the source recording and subsequently select an artist/AI voice to generate an AI cover of that recording. This enables copyright-protected recordings available through YouTube to be obtained and used as source material within the application before being processed to create a new AI-generated version using the selected voice.

The functionality raises concerns in relation to both copyright and voice, image, name and likeness (VINL) rights. In particular, the application facilitates the use of copyright-protected recordings as source material while also enabling synthetic representations of artists' voices to be applied to those recordings. Where artist voice models are provided without authorisation, users can therefore create recordings which imitate identifiable recording artists without evidence that the relevant artist or right holder has authorised either the use of the underlying recording or the cloning and exploitation of the artist's voice.

MusiQ AI should be included on the Watchlist due to the combination of its stream-ripping, AI cover and vocal cloning functionality. The ability to paste a YouTube URL directly into the application substantially simplifies the process by which users can obtain and repurpose copyright-protected music. Rather than requiring users to supply independently obtained source material, the application can access content from YouTube and use that material as the basis for an AI-generated cover incorporating a selected synthetic voice.

The application is also commercially monetised. Apple lists MusiQ as containing advertising and offers multiple MusiQ Premium in-app purchases, including a USD 39.99 Premium option. The application's version history further demonstrates continued development of its AI cover functionality, with Custom Voice for Covers introduced in April 2026.

MusiQ has a total of 50K downloads.

b) Shadow Libraries

Anna's Archive

On 20 December 2025, the shadow library Annas Archive publicly announced that they had downloaded 86 million music files from Spotify and metadata for 256 million tracks. Further data was to be released in different stages, including music files, additional file metadata, album art and zstdpatch files. The metadata database torrent file was available until 15 January 2026 following which Anna's Archive published on the four domains from which it

operated that it was "unavailable until further notice." However, on 11 February 2026, they released 3 million music files.

On 2 January 2026, RIAA and Spotify successfully obtained an emergency ex parte temporary restraining Order against Anna's Archive and as a result the site's .org domain was suspended by the domain registry PIR and Cloudflare stopped providing services to Anna's Archive. The Order remained under court seal until 16 January 2026 when the judge replaced the temporary restraining order with a preliminary injunction.

On 14 April 2026, RIAA and Spotify obtained a USD 322 million default judgment against the unknown operators of Anna's Archive. IFPI has carried out disruptive actions concerning the shadow library Anna's Archive in support of RIAA's efforts in the US including succeeding in getting five Anna's Archive domains suspended and disabling its payment services. The site has been blocked in a number of countries following applications by rights holder including in the UK, Germany, Netherlands, Italy and Belgium.

c) Mobile Apps

There are also increasing concerns in connection with piracy via mobile apps (beyond the AI apps) and the inadequacy of policies and measures adopted by app stores to tackle the issue, as internet users seem to move from browser-based piracy to app-based piracy using mobile devices.

Mobile apps remain one of the primary gateways for accessing illegal content online. App store compliance varies significantly by app type, with parasitic and stream-ripping applications continuing to present substantial enforcement challenges as they are often not being removed expeditiously.

These challenges are driven in large part by app store takedown procedures that are inefficient, unnecessarily burdensome and, arguably, not fully aligned or compliant with the applicable legislative frameworks, particularly the EU Digital Services Act ("DSA"). It is clear that the app stores should step up when it comes to tackling copyright infringements via apps that they are making available online.

Musi – Simple Music Streaming ("Musi")

Musi is an unlicensed music streaming app, based in Canada, which is currently unavailable through any mainstream app store following its removal from Apple's App Store.[6] However, the app remains accessible on Apple devices where users had previously installed it. Users who previously acquired Musi through their Apple account may also be able to reinstall or sideload the application onto an Apple device despite its removal from the App Store. Consequently, its removal does not prevent Musi from retaining an active user base. Continued access to the application also provides the developers with the opportunity to continue generating revenue from existing users, including through premium subscriptions and in-app advertising.

[6] https://apps.apple.com/us/app/musi-simple-music-streaming/id591560124

Musi obtains content, which includes copyright-protected content, from YouTube. It does this by circumventing the technical protection measures implemented by YouTube for the purpose of preventing acts which are not authorised by right holders and makes that copyright protected content available to the public without relevant authorisation. Musi has the appearance and functionality of a conventional music streaming service, providing on-demand music with search facilities and features such as the ability to organise content and build playlists, but without a licence to do so.

In August 2026, in an action co-ordinated by IFPI and its national group Music Canada, Sony Music Group and Universal Music Group commenced legal proceedings in Canada against the developers of Musi.

Musi has also been the subject of legal proceedings in the US, following Apple's decision to remove the Musi app from the App Store. Musi sued Apple alleging that the removal of the app amounted to a breach of its agreement with Apple and a breach of the implied covenant of good faith and fair dealing. However, in March 2026, the US District Court of the Northern District of California dismissed Musi's complaint with prejudice.

Why should the site be included on the Watchlist

When live on the Apple app store Musi was an extremely popular app. It had over 100 million+ downloads on the IOS store since its creation in January 2018 with approximately 2,412,059 downloads over a 30-day period. During the peak of its popularity, it was ranked seventh in the App Store's global top charts.

Musi acts as a music streaming service, akin to licensed services such as Spotify, competing with such services, but without paying or compensating right holders for the content which it is making available.

Youtify

Youtify is a music streaming application currently available on the Apple App Store and operated by developer Thai Huy Nguyen, who appears to be based in Vietnam. The app enables users to search for and stream music, import playlists from YouTube, search YouTube content and play videos as audio. Youtify is monetised through both advertising and paid Premium subscriptions, including monthly, annual and lifetime options. Evidence also links the developer to an Android application previously operating under the Youtify name, which was subsequently renamed/rebranded as Joytify – Music & Playlists, while retaining references to Youtify within its package and associated developer information. The shared developer identity and contact information indicate that the iOS Youtify and former Android Youtify/Joytify applications are associated with the same developer.

Youtify is a parasitic music streaming application which obtains and makes available content from YouTube, including copyright-protected music, through functionality that circumvents technical protection measures implemented by YouTube to control access to its content and prevent unauthorised use. The application has the appearance and functionality of a conventional music streaming service, allowing users to search for and stream music on demand, import and organise playlists and play YouTube content as audio. This enables users

to access copyright-protected content through Youtify's own interface rather than through the authorised YouTube service and associated controls. Youtify is monetised through advertising and paid Premium subscriptions, including monthly, annual and lifetime options.

Why should the site be included on the Watchlist

This application has been subject to enforcement action on both the Apple App Store and Google Play but remains available on both platforms. During the enforcement process, the developer has made changes to the app's features and functionality which have had the effect of obscuring the functionality of concern. The developer also submitted a counter-notice to Google, following which the application was reinstated. Following its reinstatement, the Android application was renamed from Youtify to Joytify, which appears to be an attempt to avoid or hinder further enforcement action.

Youtify is a highly popular application across both major app stores. On Google Play, the app has accumulated approximately 5 million total downloads, with a further 133,957 downloads in the last 30 days and has reached a highest chart position of No. 10 in the Music and Audio category. On the Apple App Store, Youtify has generated approximately 10 million total downloads, including 916,512 downloads in the last 30 days, and has reached a highest chart position of No. 2 in the Music category.

d) Stream Ripping Services

How it works

Stream ripping services enable users to make permanent copies of recordings from online streaming services. They circumvent the technical protection measures applied to protect the copyright content and enable users to download ("rip") it to their own devices. The ripped content is sourced from various music streaming platforms including, but not limited to, YouTube, SoundCloud, and Facebook.

Typically, a stream ripping service works by allowing a user to copy the URL of the content hosted on an online platform and paste the URL into a search box which appears on the homepage of the stream ripping service, which then provides the user with a media file (in MP3 or MP4 format, for example) once they have clicked the download button. In addition, stream ripping services often add metadata, such as the name of the title or the artist, to the downloaded file.

It is common for stream ripping services to further facilitate the process of stream ripping, e.g. by providing a search function on their website (so that the user does not need to search for a link on other platforms), or by promoting the most popular tracks for download directly on their homepage. Other stream ripping services even offer so-called browser extensions which result in a specific download button being placed on the online platform making it even quicker and easier for users to 'rip' content as they simply click the download button on a platform, such as YouTube, thereby avoiding the need to copy and paste the URL.

The music that these websites make available to the public has not been licensed for download or offline use, only for streaming. Moreover, the Terms of Service of services such

as YouTube that operate an ad-supported streaming model, prohibit their users from downloading the streamed content. For these reasons, YouTube has implemented a number of technical protection measures to prevent stream ripping. Stream ripping sites are circumventing these measures that enjoy legal protections under the international treaties and EU law.

As a result, stream ripping is causing substantial harm to the industry including through: (a) reducing traffic to streaming platforms, thereby reducing advertising revenues; (b) reducing sales of premium subscription streaming services, which offer offline and mobile access; and (c) diverting sales of permanent downloads.

Stream ripping services derive revenue from advertising and some services also encourage users to donate money in order to help cover the costs of running the service.

IFPI is currently tracking over 300 stream ripping sites. Some of the most popular and therefore, most damaging ones are set out below.

Since our last submission we have become aware of a new type of stream ripping site which allows users to 'rip' from certain digital service providers and upload a copy of the file to a number of cyberlockers. An example of such a site includes Lucida.to.

Following IFPI's last submission, together with our National Group in Germany, we were successful in an action we coordinated on behalf of local music right holders against an individual in Germany who was hosting the website from where the stream ripping software YouTube-DL could be downloaded. In November 2024, the Hamburg Appeal Court dismissed the defendant's appeal in its entirety and confirmed the Regional Court's decision from 31 March 2023 to issue an injunction requiring the defendant to stop hosting the stream ripping software YouTube-DL and also confirmed that the defendant was obliged to pay damages. The software had been allowing users to download content directly from YouTube, thereby circumventing YouTube's technical protection measures applied to protect licensed streamed content from unauthorised downloading. The court found the defendant liable for aiding and abetting the circumvention of technical protection measures and also liable for aiding and abetting the distribution of the circumvention software. The defendant was unable to rely upon the hosting provider safe harbour defence as he had sufficient knowledge following receipt of a cease and desist letter back in September 2020. The decision is pivotal in relation to stream ripping tools confirming their infringing nature and it also has precedential value concerning the liability of hosting providers which can face claims for damages if they have not taken sufficient action in relation to copyright infringements.

Additionally, in 2025 IFPI was able to secure the closure of Y2mate.com and eleven other stream ripping sites following targeted enforcement action in Vietnam.[7] We have however, noted that even after the enforcement action against Y2mate.com, numerous stream ripping sites continue to trade off its notoriety by incorporating 'y2mate' into their own domain to attract users. We have included two popular examples in our submission.

[7] IFPI shuts down Y2mate.com and 11 other major stream ripping sites in landmark action in Vietnam - IFPI

Y2Mate.gs (formerly y2mate.nu)

The site operates as a typical stream ripping site in that a user pastes the YouTube URL for the video, they wish to 'rip' into the box on the site's homepage and the user then selects whether they wish to download the file in MP3 or MP4 format once they've clicked on the Convert button. The site notes on its homepage that "*Y2mate is an easy way to download YouTube videos as MP3 or MP4 files. Y2mate is free to use and does not require any sign-up or subscription."* According to SimilarWeb, over the last 12 months (August 2025 to July 2026) there have been over 546 million visits to the site globally. The site is currently subject to website blocking orders in Spain, Indonesia and Brazil.

Savefrom.net[8] and ssyoutube.com

Over the last 12 months (August 2025 to July 2026) according to SimilarWeb there have been over 1.3 billion visits to Savefrom globally. To give a sense of scale, this is more internet traffic than the newspapers Le Monde (Lemonde.fr), or Le Figaro (lefigaro.fr).

Savefrom operates with a slightly different technical model to other stream ripping services, but an equally damaging one. Rather than downloading content to their servers and then offering MP3 files or MP4 files for download, Savefrom simply circumvents the YouTube content protection measures and serves up the unprotected content to users directly from the YouTube servers where the user can either save the video or save the audio to their devices.

In April 2020, the service announced that it would be discontinuing its offer in the US citing that it is no longer financially viable due to their industry being under persistent attacks from certain US copyright holders[9] (the music industry is amongst them). The service similarly discontinued its operations in the UK, Canada and Spain. However, the service continues to operate in other territories outside of the USA, UK and Spain.

Ssyoutube.com is being run by the same operator as Savefrom.net. The site is also very popular globally with over 217 million visits in the last 12 months (August 2025 to July 2026) according to SimilarWeb. Both savefrom.net and ssyoutube.com provide step by step instructions on its homepage as to how users can 'rip' content via the site.

As the site operator is based in Russia, website blocking orders are currently the most effective method to impact these sites. Following music right holders' actions, Savefrom.net is currently subject to website blocking orders in Brazil, Denmark, India, Indonesia, Italy, Paraguay, Peru and Spain and ssyoutube.com is blocked in Brazil, Indonesia, Italy, Paraguay, Peru, and Spain. However, more blocking actions are needed to limit the availability of both sites throughout the EU and the injunctions should be sufficiently flexible to allow for future domains of the same service to be blocked in short timeframes.

[8] Sfrom.net automatically redirects users to savefrom.net
[9] https://us.savefrom.net/

Y2mate.is

Y2mate.is operates as per Y2mate.gs by allowing users to paste the URL for the YouTube video they want to 'rip' into the box on the site's homepage and press Start following which the user can download the file in MP3 or MP4 format. The site provides step by step instructions on its home page as to how users can download YouTube videos via the site and how their service differs from others. The site emphasises the service is free, converts YouTube videos quickly and there is no limit on the number of videos a user can convert each day. According to SimilarWeb, over the last 12 months (August 2025 to July 2026) there have been over 99 million visits globally to the site. Following music right holders' actions Y2mate.is is currently subject to website blocking orders in Brazil, France, India, Indonesia, Italy, Mexico, Peru and Spain.

YTDL-P

YT-DLP is an open-source command-line application written primarily in Python. It automates the retrieval of video, audio and associated metadata from supported online platforms by processing supplied URLs, issuing HTTP requests, parsing webpage and player data, and interacting with platform-specific playback endpoints. The tool is widely used to extract or "rip" audiovisual streams from digital service platforms, including YouTube and numerous other supported services.

Github is YT-DLP's official source; it serves as the main platform for accessing the scripts latest updates, source code, pre-compiled binaries and installation instructions. However, YT-DLP has been redistributed on other software repositories such as PYPI.ORG[10] and existing copies and forks can also be found on third-party websites.

On GitHub, the repository is described as a "feature-rich command-line audio/video downloader." The YTDL-P fork was publicly launched in 2021, and the core source code is released under The Unlicense, permitting users to use, modify and redistribute the software. This has enabled the project to attract a large global community of developers who actively maintain and improve the application. YTDL-P is a fork of the youtube-dl project, which was originally released in 2006. In summary, YTDL-P originated from the same codebase as youtube-dl but has since diverged significantly through the introduction of new features, additional platform support and bug fixes that were not incorporated into the original project. As both repositories are open source, developers have been able to build upon the existing codebase while complying with the project's licensing terms. As of July 2026, the official GitHub repository has approximately 14,400 forks, more than 179,000 stars, around 1,900 contributors, over 110 releases, and the latest stable release is version 2026.06.09.[11]

YT-DLP does not have a single sole developer and is maintained as a community-driven open-source project with contributions from a large international developer community. The fork was originally created by the developer using the username "pukkandan", who served as the lead maintainer between 2021 and 2024.[12] The project is now maintained by a team of core

[10] https://pypi.org/project/yt-dlp/
[11] https://github.com/yt-dlp/yt-dlp/releases
[12] https://ytdl-org.github.io/youtube-dl/about.html

maintainers,[13] including users operating under the usernames "coletdjnz", "bashonly" and "Grub4K".

YT-DLP is a major problem for the music industry as it provides freely available open-source software that enables users to download and permanently store music and audiovisual content from licensed streaming platforms, including YouTube, without authorisation. Its open-source nature, extensive developer community and its widespread distribution results in the tool being difficult to contain and/or remove, while continuing to facilitate stream ripping at scale and depriving right holders, artists and licensed services from legitimate streaming and downloads.

e) Cyberlockers

How it works

A "cyberlocker", also known as a "one click file-host", typically refers to a type of file-sharing website. They enable users to distribute links to digital files uploaded and stored on an online storage infrastructure that is controlled, managed and maintained by the website's operator. These types of services are highly secretive about their corporate ownership, often utilise offshore shell companies and domain privacy services to mask the identity of their officers, and thus behave, in this and other ways, differently from legitimate providers of cloud storage services. Therefore, it can be extremely difficult to take direct actions against this type of pirate service. Some cyberlockers claim to operate a "DMCA" takedown policy and remove content in response to takedown notices sent by right holders. However, when it comes to the cyberlockers which are a concern for the music industry, it should be noted that – if at all – the DMCA could only apply in the US. Under EU legislation, by contrast, most of these cyberlockers would probably not be entitled to safe harbour protection in the first place (the relevant question would be whether they are directly or indirectly liable) and thus the question whether or not they comply with a takedown request should be irrelevant. Instead, they should take effective and meaningful steps to ensure that infringing content does not appear on their service.

On 22 July 2021, the CJEU handed down its decision in the joined proceedings against Uploaded – a cyberlocker – and YouTube (C-628/18, C-683/18). The CJEU provided a non-exhaustive list of factors and examples that it considered indicate that a cyberlocker is communicating works to the public, and therefore needs a licence.[14]

[13] https://github.com/yt-dlp/yt-dlp/blob/master/Maintainers.md

[14] i) where that operator has specific knowledge that protected content is available illegally on its platform and refrains from expeditiously deleting it or blocking access to it; OR - where that operator, despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform; OR - where that operator participates in selecting protected content illegally communicated to the public; OR - provides tools on its platform specifically intended for the illegal sharing of such content or knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform.

Key features commonly displayed by cyberlockers, which are designed to facilitate the distribution of infringing content at scale, include:

a. **Premium accounts**: Paid premium accounts which provide the user with increased storage, quicker download speeds, and unlimited downloads. In some cases, the user must purchase a premium package to download content from the site, while other sites promote premium accounts but also offer a free download option. Domains (i.e. indirect download sites) may also redirect a user to cyberlockers which subsequently require the purchase of a premium package to complete the download process. This is a method for operators of the referral sites, to make revenue via commission from the cyberlocker.

b. **Incentive/revenue-sharing schemes:** Schemes which reward high-volume downloading and/or offer incentive schemes for uploaders. Such features may include PPD (pay per download) or PPS (pay per sale).

c. **Unrestricted, sharable links**: Most cyberlockers provide users with shareable links for content uploaded to the site. This facilitates the distribution of infringing content as the material can be easily accessed by anyone with the link.

d. **Short retention period**: Deletion of inactive files after a short period of time, such as 30 or 60 days, which would be unsuitable for permanent, private storage.

e. **Role in pre-release piracy, including via "Group Buys":** Certain cyberlockers are frequently used to distribute snippets – or full versions – of leaked, pre-release content. This includes during the course (or at the successful completion) of a Group Buy. A Group Buy is the sale of unreleased music content, which is offered on a platform such as a private Discord server/channel. The target selling price is set by the organiser of the sale and met through donations from users taking part, all of whom receive a copy of the leaked content when the target price is reached.

f. **Encryption methods**: Cyberlockers may use encryption techniques for stored content, for example, using the Advanced Encryption Standard (AES) algorithm. On a cyberlocker, this may consist of a user having an encryption key for each file uploaded, which is then encrypted with the user's personal key which is stored on the site's server. Therefore, the only unencrypted content on the site's server is a user's encryption key. This allows the user to maintain their account security and privacy in respect of uploaded content, whilst also being able to share files with other users.

g. **Privacy protection measures**: Operators of cyberlockers ensure their identities are hidden, such as masking domain registrant details with privacy protection services and making use of bullet-proof hosting providers that do not respond to requests from right holders to disclose contact details of clients that use their services for infringing activity.

Trends in cyberlocker piracy

Cyberlockers have been a major music piracy threat for nearly two decades. Uploaders of content are frequently offered the ability to profit from the files added to a cyberlocker while downloaders find a wealth of unlicensed material via a one-click download. As explained above, cyberlockers themselves make money through advertising and payments for 'premium' accounts that give uploaders more space to store files and other users faster and unrestricted downloads.

Following the closure of MegaUpload, one of the most notorious cyberlockers, a major international law enforcement operation produced a gradual long-term decrease in the overall use of cyberlockers, though lockers remained one of the most popular piracy methods.

However, in addition, and as described above, cyberlockers remain a major distribution channel for leaked pre-release content. The piracy networks which make available material before its licensed release date, the period during which it will make the most economic harm, typically use cyberlockers to host and distribute the files. A key reason is the anonymity they provide for uploaders and downloaders.

Due to its exclusive nature and difficult access, pre-release piracy remains a major concern for the music industry. Not only does pre-release piracy impact the producers of phonograms but also the very many people that are involved in the process of conceiving, creating and promoting the release; critically, this includes the artist, who is deprived of the ability to control his or her own narrative around the release. This role gives added importance to cyberlockers within the music piracy landscape.

Ddownload.com (ddl.to and download.to redirect to Ddownload.com)

Ddownload.com continues to be a problematic cyberlocker for the music industry. The service is available online and is also available as an app. The service was listed in the EU Counterfeit and Piracy Watchlist 2022 and 2024, and it plays a key role in the music piracy ecosystem, specifically in relation to the making available of pre-release music content i.e. music which has yet to be commercially released. As such its activities are particularly damaging to IFPI members and artists. Links to content stored and made available via this cyberlocker are frequently found on websites promoting access to infringing content, including pre-release content such as scnlog.me, and goldesel.bz.

Ddownload makes revenue via premium packages which provide features such as increased storage, quicker download speeds, and unlimited downloads. The site also actively promotes discounted premium packages. Multiple file types can be uploaded onto Ddownload.com.

While the operator(s) remove infringing content from the platform on notification by right holders, the service does not take measures to prevent or deter the uploading of infringing content to the platform and consequently, notified content reappears on the platform. IFPI has observed the cyberlocker changing hosting provider following disruptive enquiries.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026), Ddownload.com has received over 51 million visits globally. The site receives over 29 percent of its traffic from

Germany and over 33 percent of its traffic from Japan. Other countries in the EU including Austria and Spain, are listed within the top ten countries that the site obtains traffic from.

Pillows.su

Pillows.su is another popular cyberlocker which is detrimental towards the music industry due to its use in connection with the distribution of pre-release content. This cyberlocker emerged when the cyberlocker onlyfiles.io whose operator was heavily involved with the distribution of pre-release content, went offline in February 2023. The site initially appeared as a mirror site of onlyfiles.io.

Links to infringing content hosted on Pillowcase.su are frequently found on known leak sites and forums, including Leaked.cx (of which it is a preferred/allowed hosting provider for posted content, and is its top referring website), lanaboards.com and sharemania.us.

This cyberlocker makes available copyright-protected content to the public without authorisation from copyright holders and derives revenue from advertising.

The operator(s) of Pillowcase.su have purposively taken steps to conceal their identities by for example, using domain privacy protection services and by obtaining hosting services from Khomutov Artem Sergeevich in Russia.

This cyberlocker was previously accessed via Pillowcase.zip which then redirected to Plwcse.top, where all infringing content on the site was hosted. Pillowcase.su was also used to access the service and did not redirect users to another URL. These domains are no longer active, and the service now solely operates through Pillows.su, where the infringing content is hosted.

The service is unresponsive to infringement notices, with an estimated 0.3 percent compliance rate from 2026; this means that leaked content shared on the service can proliferate unabated.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026) Pillows.su has received over 9 million visits globally. The site receives over 59 percent of its traffic from the USA and over 4 percent of its traffic from the UK. Some EU countries including for example Germany, France Italy and Poland are listed within the top ten countries from which the site is receiving traffic.

Mega.nz/.io

Mega is a popular cyberlocker which is used in the distribution of infringing music content, including pre-release content. Its ease of use, structure and focus on privacy makes it a popular cyberlocker for such use. Mega was included in the 2024 EU Counterfeit and Piracy Watchlist.

Mega is operated by Mega Limited, located in New Zealand. Some of its current – and former – company officers have included individuals involved with the notorious cyberlocker Megaupload, of which Kim Dotcom was the founder. The US criminal investigation against

Kim Dotcom remains pending along with civil actions filed by the film and music industry. In 2015 Kim Dotcom, revealed he was no longer associated with Mega.nz or the Mega company. However, the controlling company of Mega Limited is Cloud Tech Services Ltd located in Hong Kong. Kim Dotcom is listed as a historic shareholder for this company and currently the largest shareholder is the Dotcom family Trustees Limited.

Mega also has both Android and iOS mobile applications.

At the time of writing, the Mega website claims to have over 352 million plus registered users in 200 plus countries and promotes itself on the basis of its privacy features, including user-controlled end-to-end encryption. In order to register for a free account, all that is required is a first name, email address and a password. A key feature of Mega is that it allows account holders to transfer content directly between accounts, which makes sharing content much quicker. Once content has been shared in this way, each copy needs to be reported for removal separately. Accordingly, infringements can easily proliferate within the site, making detection and removal more difficult to manage.

Mega allows users to create a Mega Cloud Storage, also known as Mega folders, in which uploads of up to 20 GB can be made without paying for a subscription. In addition, Mega offers "MEGA achievements" that provide the user with different perks such as free storage when they complete a set of tasks such as inviting friends to the service, or installing one of their services. In addition, Mega earns revenues through a range of paid subscription plans for individuals and businesses. Paid subscriptions for individuals provide the user with higher amounts of storage. 'Mega for Business' allows a team to share an account of up to 300 members; give users administrator status; and share files amongst the server. There are also a variety of storage options to choose from, i.e. 20 GB with a free account or between 200GB and 20 TB with a paid account.

Therefore, Mega attracts customers with free, secure cloud storage with a focus on privacy; and to subsequently charge a cost for further premium subscription packages to enhance the user's experience.

More recently, we have seen Mega used to host AI vocal models and share via platforms such as Discord referenced later in our submission.

<u>Compliance and relevant actions taken</u>

Mega has received thousands of infringement notices from the recorded music industry. While the operators of Mega remove infringing content from the platform that is notified to it by right holders, the service does not apply content filters to prevent or deter the uploading of infringing content to the platform. Mega should be required to take more effective measures to prevent infringements on the platform.

In January 2022, ISPs in Russia were ordered to permanently block the site following music rights holders' actions. However, the block was lifted following an appeal.

In July 2026, IFPI sent a cease-and-desist letter to MEGA concerning the large volume of infringing and pre-release music available through the service and requested stronger

measures to prevent repeat infringements. MEGA responded that it operates a notice-and-action system and repeat infringer policy but does not proactively monitor user content or prevent future uploads of reported works. The company cited its end-to-end encrypted service as limiting its ability to identify infringing content without specific notifications from rightsholders.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026) Mega.nz has received over 1 billion visits globally. The site receives over 11 percent of its traffic from the USA and over 3 percent of its traffic from Spain. Other countries in the EU including Germany and France are listed within the top ten countries that the site obtains traffic from. To give a sense of scale, this is greater global internet traffic than to the domains of Adidas (Adidas.com), or Dior (Dior.com).

Historically, the domain's TLD regularly alternated between Mega.nz and Mega.io. However, Mega.nz automatically redirects users to Mega.io which has received over 53 million visits during the last 12 months and is most popular in the USA with over 10 percent and Spain with over four percent of traffic. Other countries in the EU including Germany and Italy are also listed within the top ten countries that the site obtains traffic from. Users now browse the Mega.io front-end, but all infringing content is hosted by the Mega.nz domain.

Turbobit

Turbobit.net has been a long-standing problem for the music industry, making available infringing content including pre-release content. It allows users to upload up to 100 GB of content and provides users with a link where they can further share infringing content on other platforms.

Turbobit is used by linking sites, such as themusicfire.net, getrockmusic.net, and losslessmusics.org to store/host copyright infringing files. Turbobit derives revenue from premium accounts and advertising placed on the site. Premium packages provide features such as increased storage, quicker download speeds, and unlimited downloads. Add-on packages are available to purchase which allow the user to upload content anonymously. Turbobit.net has an associated domain which is Turbobit.me, which promotes the site. When accessed, a pop-up message is displayed, stating that if users pay once for a premium account, they will gain access to unlimited downloads from +60 file hosting sites; if clicked on, the user is redirected to the packages page at Turbobit.net, but the specifics as to the services it is referring to are not provided.

The domain is responsive to reports of infringements on its platform; with an estimated 95.9 percent compliance rate from 2026. However, it does not take preventative measures such as content filters or warnings presented to the user when attempting to upload infringing content on the domain.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026) Turbobit.net has received over 62 million visits. The site receives over 13 percent of its traffic from Turkey and over 9 percent from Germany. Other countries in the EU, including Spain, Poland and France are listed within the top ten countries that the site obtains traffic from.

Rapidgator

Rapidgator.net continues to be a problematic cyberlocker for the music industry. The service was included in the EU Counterfeit and Piracy Watchlist in 2022 and 2024, and it plays a key role in the music piracy ecosystem, specifically in relation to the making available of pre-release music content. As such its activities are particularly damaging to IFPI's members and artists. Rapidgator was included in the 2024 EU Counterfeit and Piracy Watchlist.

Rapidgator derives revenue from premium accounts. Premium packages provide features such as no ads displayed to the user, quicker download speeds, and unlimited downloads. Rapidgator also offers reward schemes that incentivise sharing and downloading content on the site. Via the associated domain Rapidgators.net, there is a section detailing how users can make money under different reward schemes with various reward rates. The Rapidgator reward schemes are categorised as "pay per download" (PPD), and "pay per sale" (PPS). For PPD, they claim that the user can receive payments for when their files are downloaded 1,000 times by other users, and the reward provided is dependent on the size of the files and the country from which they are downloaded. For PPS, they claim the user can get 50 percent of the purchased premium accounts and 50 percent from rebills. They also state that users can earn revenue when they distribute their affiliate link, and other users register to the cyberlocker with it.

Rapidgator complies with takedown notices, with an estimated 88.9% percent compliance rate for 2026. However, the site contains a high amount of member-owned content, and the operator does not take measures to review the content uploaded to their site, to avoid infringing content being distributed via their service.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026) Rapidgator.net has received over 302 million visits globally. The site receives over 43 percent of its traffic from Japan and over 8 percent of its traffic from Germany. Other countries in the EU including France and Spain, are listed within the top 20 countries that the site obtains traffic from.

Imgur.gg

Imgur.gg is another popular cyberlocker which is detrimental towards the music industry due to its use in connection with the distribution of pre-release content. Links to infringing content hosted on Imgur.gg are frequently found on known leak sites and forums, including Leaked.cx (of which it is a preferred/allowed hosting provider for posted content, and is its top referring website), sharemania.us, pophateflops.com, and lanaboards.com.

This cyberlocker makes available copyright-protected content available to the public without authorisation from copyright holders.

The operator(s) of Imgur.gg have taken steps to conceal their identities. The service provides only limited contact information through email addresses associated with the cpa.gg domain, which do not reveal the identity of the operator. An associated social media presence exists but restricts public access to account information.

Technical analysis indicates that the service uses a layered hosting setup involving Cloudflare, Netlify and Amazon Web Services (AWS), making it difficult to identify the operator or underlying infrastructure. The domain is registered through Namecheap. All intermediaries referenced are based in the USA.

Imgur.gg has experienced repeated periods of downtime and has previously directed users to a backup service, temp.imgur.gg, when the primary domain was unavailable. Despite these outages, the service remains a popular hosting platform within leak communities and continues to be used for the distribution of infringing content.

The operators of this cyberlocker created the site Unrlsd.app in June 2026. It is a platform designed for hosting and sharing unreleased music, which enables users to create playlists and distribute audio files via downloadable links. It is not currently popular and has low traffic.

Compliance testing conducted in 2026 suggests that Imgur.gg is inconsistent with infringement notices i.e. the site does not respond to take down notices, with only an estimated 27.6 percent compliance rate.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026) imgur.gg has received over 2.5 million visits globally. The site receives over 51 percent of its traffic from the USA and over 6 percent of its traffic from the UK. Other countries in the EU including Germany, Poland and the Netherlands, are listed within the top ten countries that the site obtains traffic from.

Pixeldrain.com

Pixeldrain.com has become a problematic cyberlocker and has previously been linked to other services. In reference to the cyberlocker Dbree.org, IFPI observed Dbree.org redirecting to Pixeldrain.com over a short period of time between August 2025 to March 2026. Other sites which are part of the Dbree network also redirected to Pixeldrain.com. A connection between the operator of Dbree.org and Pixeldrain.com could not be made at the time. Despite this, the redirection suggests an affiliation with the service purposely distributing infringing content including pre-release.

Links to infringing content hosted on Pixeldrain.com are frequently found on known leak sites and forums, including Leaked.cx (of which it is a preferred/allowed hosting provider for posted content, and is its top referring website), sharemania.us, scnlog.me and doubledouble.top. This cyberlocker makes available copyright-protected content to the public without authorisation from copyright holders.

The operator(s) of Pixeldrain.com have not taken steps to conceal their identities. The service provides links to other social platforms such as Discord, Patreon, Reddit, GitHub and Mastodon. Pixeldrain is a product by Fornaxian Technologies. The exact location of the company and developer is yet to be determined.

The cyberlocker also offers an Android app for uploading and sharing files on Pixeldrain. The APK is available to download from the service's connected GitHub profile.

Compliance testing conducted in 2026 suggests that Pixeldrain.com is compliant with infringement notices i.e. the site does respond to take down notices, however an estimated compliance rate could not be determined.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026) Pixeldrain.com has received over 473.5 million visits globally. The site receives over 13 percent of its traffic from the USA and over 10 percent of its traffic from Indonesia. Other countries in the EU including Germany, France and the Netherlands, are listed within the top ten countries that the site obtains traffic from.

f) BitTorrent Indexing Sites

Trends

BitTorrent remains a noticeable issue for music piracy. While BitTorrent is primarily used to download pirated film and television content, large stocks of music are also available on most BitTorrent sites such as 1337x and The Pirate Bay – all services listed in the 2020, 2022 and 2024 EU Counterfeit and Piracy Watchlist. These services remain a problem for our sector and should continue to be listed. A unique feature of BitTorrent is the availability of full artist discographies: with a single click, a BitTorrent downloader can obtain the entire catalogue of The Beatles, Taylor Swift, BTS, or many other artists. In this way, the harm caused by BitTorrent can outweigh the relatively lower levels of visits compared to other categories of pirate sites.

BitTorrent sites, including 1337x and The Pirate Bay have been blocked in many EU countries, but not right across the EU, which illustrates the need for cross-border injunctions or other mechanisms allowing an easy and cost-effective pan-European enforcement response.

g) MP3 Download Sites

'Muz' network

Over the last year, IFPI have identified a number of sites using the prefix 'Muz'. In Russian, муз- (muz) is the standard prefix used for anything related to music (for example, muzykalny means musical). Web developers and site creators often use "muz" in domain names as a catchy, short abbreviation to signal that the website is a music library, streaming platform, or MP3 download archive. In this instance, these sites have a similar interface; presented in Russian and designed to easily download content in mp3 formats. Popular sites include Muzcha.net and Muzyet.com.

Content made available across the sites is predominately Russian and international artists. The sites have a simple interface and are dedicated to sharing music files. These websites also support malicious site advertisements that have been reported as downloading malware.

Compliance testing conducted in 2026 suggests that Muzcha.net does respond to take down notices. Muzyet.com however, is inconsistent with infringement notices with only an estimated 34.1 percent compliance rate.

Two of the more popular sites within the network include Muzyet.com and muzexo.net which have received 4.5 million and 8.9 million global visits respectively. The most popular countries for these sites are Russia, Ukraine and Kazakhstan.

h) Nigerian Download Sites

Ceenaija.com

Ceenaija.com has emerged as a popular infringing site across Africa. Similar to other problematic MP3 download sites in Africa, the site is receiving the highest level of traffic from Nigeria. As of August 2026, the site delivered content as an indirect download, with content being hosted on a bespoke domain. The site generates revenue from advertisements.

The site predominantly distributes gospel repertoire but does have a dedicated page for international artists. The gospel genre has moved beyond traditional means of consumption and into mainstream media, concerts, and digital platforms. Thousands of links have been reported against the site since 2020.

Compliance testing conducted in 2026 suggests that Waploaded.com is inconsistent with infringement notices i.e. the site largely does not respond to take down notices, with only an estimated 55.8 percent compliance rate. The site has been subject to disruptive actions without success.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026), Ceenaija.com has received 41.29 million global visits. Over this period, the site received over 64 percent of traffic from Nigeria. Other popular countries included Ghana and South Africa.

Trendybeatz.com

Trendybeatz.com is a prolific infringing site, popular in African countries, particularly Nigeria from where the site is operated. The site has now established itself as one of the most popular MP3 download sites in Africa. As of August 2026, the site delivered content as a direct download, with the content being hosted on the domain. The site generates revenue from advertisements through third parties and offers for users to contact the operator to assist with advertisement placement.

Although the site largely focuses on African repertoire, it also makes available international repertoire. A search bar allows users to target their desired content. The site also offers a Music News and Reviews page. They have also established a channel on Telegram. Since 2021, thousands of links have been reported against the site, and the high levels of traffic make it a concern for the region.

Compliance testing conducted in 2026 suggests that the domain is non-compliant with infringement notices i.e. the site does not respond to take down notices, with only an estimated 1.9 percent compliance rate. The site has been subject to disruptive actions without success or action taken by the operator.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026), Trendybeatz.com has received 40.71 million global visits. Over this period, the site received over 70 percent of traffic from Nigeria. Other popular countries included Ghana and South Africa.

Waploaded.com/Meetdownload.com and related sites

Waploaded.com and related sites are a network of prolific infringing sites which are popular in Africa and are operated from Nigeria. As well as offering music as MP3 downloads, the site offers pirate movies and IPTV. Since 2023, IFPI have reported thousands of audio links against the site. As of 2026, the site is more popular for downloading and accessing films and television series compared to music. As of August 2026, Waploaded.ng and Waploaded.com.ng are also active sites and redirect users to Waploaded.com. Waploaded.com is a linking site which directs users to download content from Meetdownload.com. The site is directly connected to Waploaded.com and content is served from the domain. Although the site is presented as being similar to a cyberlocker, users are not able to upload their own content. The site generates revenue from advertisements through third parties and encourages users to contact the operator to assist with advertisement placement.

Waploaded.com provides different audio categories for users to explore, including South African and Nigerian repertoire. International repertoire has become less accessible and we are aware that the site now displays a message on the 'Foreign HipHop songs' section of its site noting that the content on this page has been permanently removed. The Nigeria-based operator openly promotes the network across their own social media channels. The business model is presented as a legitimate business despite making available infringing content. A Nigeria registered company was discovered in connection with the network.

Compliance and relevant action points

Compliance testing conducted in 2026 suggests that Waploaded.com is inconsistent with infringement notices i.e. the site has an estimated 55 percent compliance rate with takedown notices. Meetdownload.com however is non-compliant with infringement notices and had an estimated 1 percent compliance rate. The site has been subject to disruptive actions without success.

According to SimilarWeb, in the last 12 months (August 2025 to July 2026), Waploaded.com received 24.58 million visits globally. Over this period, the site received 53 percent of visits from Nigeria and 16 percent from South Africa.

Hiphopkit network

Hiphopkit.com is a prolific infringing site that is popular in African countries and operated from Nigeria. A number of sites that share a similar design and offer infringing content are connected to the same operator, including Justnaija.com and hiphopkit.com. Since the last submission in 2024, IFPI has identified 11 sites as part of the network. In August 2026, the majority of these sites are no longer active. However, Justnaija.com and hiphopkit.com remain popular across Nigeria and Africa. The operator of the Hiphopkit network receives revenue from advertisement.

Content made available across the network relates to African hip hop music. Although the site largely focuses on African repertoire, international repertoire has also been made available. All sites have a social media presence and advertise their channels across Facebook, Instagram and X/Twitter. Additionally, WhatsApp phone numbers are provided as users are encouraged to request songs via this channel.

Compliance testing conducted in 2026 suggests that the domain, Hiphopkit.com, is non-compliant with infringement notices i.e. the site largely does not respond to take down notices, with only an estimated 7.4 percent compliance rate. The sites have also been subject to disruptive actions without success.

Justnaija.com and hiphopkit.com received 12 million and 10.4 million global visits respectively from August 2025 to July 2026. Both sites are extremely popular in South Africa and Nigeria.

Tubidy.cool

Tubidy.cool is an indirect download site[15] that enables users to watch, stream, download and upload content. Content is provided in both MP3 and MP4 formats. The site does appear to present features commonly seen on stream ripping sites, as MP4 videos to download are provided alongside audio file formats such as MP3. However, when examining the network traffic, there are no indications to suggest content is being sourced from YouTube. This suggests that the 'ripping' may be done by users or operators prior to uploading the content to the site.

Tubidy.cool blocked access to the site from the UK following receipt of a cease and desist letter from IFPI in February 2021. Further testing in 2026 has revealed that you can now access the site from the UK, however the site appears to detect and block some VPN connections.

To access the infringing content, no subscription or payments are required. If users wish to upload content to Tubidy.cool, they must create an account. Search functionality is available and the site also suggests certain content to viewers through pages such as 'Top Videos', 'Top Searches' and on the Homepage. As of August 2026, to view or download content from the

[15] An infringing website delivery method is defined as indirect download when the content is not hosted on the same domain. Even though the user remains on the same website when downloading the content, a separate domain or service hosts and delivers the content.

site, users are redirected to a secondary domain (d367.d2mefast.net, although the prefix of this domain changes frequently).

Tubidy.cool is part of a network of sites all operated from South Africa that offer the same services. However, the domain name for these sites frequently changes which we presume is a deliberate attempt by the operator to circumvent any actions taken against the site. The site has been subject to website blocking actions in Brazil and Peru.

According to Similarweb Tubidy.cool received over 21 million visits globally between August 2025 to July 2026. The top five countries sending traffic to the site over the same period include South Africa (63.20 percent), Kenya (14.07 percent), Ghana (6.75 percent), (Nigeria 3.47 percent) and Guatemala (3.22 percent).

Between July 2025 and July 2026 IFPI reported 5,270 links to the site for removal but the site failed to comply with our notices.

i) Streaming Fraud

How it works

Streaming fraud involves the creation of 'plays' on digital music streaming services ("DSPs"), such as Deezer, Spotify, SoundCloud and YouTube, by way of example, which do not represent genuine fan engagement. The artificial 'plays' are typically generated through automated means such as botnets but can also utilise cheap labour. The DSP accounts used can be created for the purpose of fraud or be hijacked from genuine customers, which could involve malware and use of stolen credentials.

Streaming fraud is part of a wider phenomenon of online fraud, which extends, inter alia, to the offering of fake comments, fake likes, fake subscribers/followers and other interactions on DSPs and on social networks more generally.

There is also a thriving business model which generates revenues by enabling streaming fraud. This includes thousands of consumer-facing services that sell fake plays and other types of engagement ('resellers). These resellers are powered by 'wholesalers' that provide the technical and business infrastructure to the resellers. By offering 'fraud as a service', resellers can start a streaming fraud enabling service with zero experience or technical expertise.

Streaming fraud has been found by courts in several jurisdictions to amount to fraud, a violation of unfair competition law and breach of consumer protection laws. It has a number of negative consequences, including the following:

- **Diversion of royalty payments**: Since DSPs pay royalties from a fixed pool, streaming fraud diverts royalties away from legitimate artists and right holders.

- **Distortion of streaming data and harm to consumers:** Fraudulent plays do not represent actual listening or genuine fan engagement. Therefore, artificial plays can distort the accuracy of streaming data. This in turn can mislead consumers and affect

the music that is curated and suggested to them. This can also impact the music charts, which are designed to reflect fan engagement and celebrate artists' success.

The operators of streaming manipulation services offer artificial 'plays' and other interactions in exchange for payment and are therefore directly generating revenues from this unlawful activity.

Artificial intelligence can be used to generate vast amounts of content that is uploaded to platforms, and the fake plays are spread across that content in order to evade detection. Technology can also be used to automate these workflows and make them harder to detect.

JustAnotherPanel.com (JAP) and Perfectpanel.com

Justanotherpanel.com (JAP) is a streaming fraud enabler service, which offers, for a fee, the generation of artificial streams or 'plays' on DSPs such as Spotify, Soundcloud, Apple Music and YouTube, with various packages available for purchase. In addition, it offers users the ability to purchase other artificial interactions (such as likes, followers, subscribers etc.) on other online platforms, including the social media platforms Instagram and Facebook. Additionally, resellers are able to access its services via API.

Other sites have been purposely designed to assist customers create their own site as resellers. Perfectpanel.com offers resellers the tools and technology to operate their own 'panel' from which they are able to sell fake plays and other types of engagement to consumers. This operation facilitates a network of streaming fraud resellers which share the same underlying infrastructure.

The location of the operators is unconfirmed, but it is believed to be outside the EU.

Why should they remain on the Watchlist

Streaming fraud is generally of significant concern to the industry because, as explained above, it diverts streaming royalty payments away from artists whose music is genuinely played, and it can also undermine the accuracy of charts and has the potential to distort consumers' impressions and understanding of the popularity of tracks and their use and enjoyment of streaming services, including by influencing algorithmic playback results.

The provision of artificially generated streams, regardless of the method of creation, also breaches the terms of service of major music streaming services. This activity can lead to both criminal (fraud) and civil liability for the perpetrator in several territories. This has been seen by several courts in Germany having ordered streaming fraud resellers to cease offering music related services on the basis that their activities violate unfair competition law, and actions by law enforcement in Brazil has resulted in the closure of dozens streaming manipulation services on the basis that they breach consumer protection law.

JAP itself has also been the subject of legal action. It was subject to a criminal blocking action in Brazil which impacted of over 1,000 related domains.[16] Recently a French court ordered OVH to terminate hosting services to JAP and a related reseller site.[17]

However, the JAP network remains resilient, and its operators continue to evade direct action. It remains the most significant player that we have identified in the global streaming fraud landscape, with over 1,000 connected domains. According to SimilarWeb[18] JAP received 6.2 million visits in the 12 months from September 2025 – August 2026. JAP exploits gaps in the legitimate streaming value chain and perpetuate an economy in fraud. Disrupting large, organised networks will have the biggest impact on the landscape.

j) Social Media With Infringing Functionalities:

Social media services are used extensively by the music industry to promote artists and facilitate direct engagement with fans. However, over the years, we have seen the emergence of social media services or platforms through which users can readily share and distribute infringing content. As confirmed by the EU Intellectual Property Office in its 2021 report, entitled "Monitoring and analysing social media in relation to IPR Infringement Report", social media platforms are used for conversations regarding infringing digital music content, and specifically by users seeking access to pirated music.

Social media and other user-uploaded content services often seek to rely on "safe harbour" protections, but the EU framework now makes clear that many such services are directly engaged in copyright-restricted acts and cannot avoid responsibility where infringing content is made available on their platforms. Under the DSM Directive, Online Content-Sharing Service Providers must obtain licences or ensure that unlicensed music content is not available, while the Digital Services Act imposes broader obligations on intermediary services, including notice-and-action procedures, trusted flagger mechanisms, repeat infringer policies and, for Very Large Online Platforms, systemic risk assessment and mitigation duties. These rules are particularly relevant to social media services, cyberlockers and other platforms with infringing functionalities, yet many services — especially those accustomed to US safe harbour standards — still appear not to have adapted their EU-facing operations or compliance practices.

X (formerly Twitter)

X is a global social networking platform which allows users to post, repost, search for and discover text, video and linked content, including through algorithmic recommendations and AI-driven features such as Grok. In the last 12 months, X.com attracted more than 52 billion visits globally. The service is monetised through advertising and reported revenue of around USD 2.5 billion in 2024.

[16] https://www.ifpi.org/brazilian-authorities-launch-largest-ever-disruption-operation-against-major-streaming-fraud-platform-justanotherpanel/
[17] https://www.ifpi.org/with-french-court-ruling-music-companies-send-strong-message-to-businesses-enabling-streaming-fraud/
[18] www.similarweb.com

Tweets can include text, hosted content such as videos, and URLs that link to external sites. X offers a highly organised service and search functionality, which all allow users easily to find and be served with content of interest. The service also relies on its AI driven "For You" algorithm and its Grok chatbot.

The platform generates revenues, including from advertising of goods and services. X's technology platform and information database enables it to provide highly sophisticated targeting capabilities for advertisers. It has been reported that X generated USD 2.5 billion revenue in 2024.[19]

Why it should remain listed on the Watchlist

X remains a significant concern for the music industry because it is widely used to share infringing music content, including hosted audio/video, links to external infringing services (e.g. to cyberlockers such as Mega referred to above, or Discord) and pre-release material. The platform's scale, reposting functionality, search tools and algorithmic recommendations enable infringing content to be disseminated rapidly and at large scale, while infringing services also use X to market their sites and notify users of newly available content. X is also used to share AI-generated content, including AI covers and other outputs that may infringe artists' voice, image, name and likeness rights. Due to the social nature of X, its volume of users and ease of access, the platform can be, and is used to share and distribute infringing content, including pre-release content, rapidly and on a massive scale; the ability to re-tweet serves to amplify the damage that is caused by such infringements. X is also used to share links to infringing websites or services from which infringing music content, including pre-release content, can be accessed. Further, many infringing services, including Mega.nz/io and Waploaded.com[20] (all discussed above) use X as a marketing platform, either to advertise their website domain to users or to notify users of new content added to their websites by including links on their associated X feed. These activities reach a large audience, thereby driving new users and more traffic to the infringing service.

Recent notice data confirms that X continues to host or facilitate access to substantial volumes of infringing content. Between January and August 2026, certain popular tracks were notified hundreds of times over the same period. X's latest compliance position remains mixed: copyright notice compliance is now reported at 87 percent, but VINL compliance remains materially lower at 61 percent, and X does not appear to take effective steps to prevent notified content, or materially similar infringements, from reappearing. X also charges right holders for API access needed to search for infringing content at scale, while continuing to benefit from a platform on which large volumes of repeat infringements occur.

What is more, unlike any other platform, X charges right holders' large amounts of money for the ability to search for tweets on its API that include or link to infringing content, at scale and without a time limitation. In other words, X is not only outsourcing to right holders the task of trying to remove IPR infringements from its platform but is also generating revenue thanks to the presence and large volume of repeat infringements on its platform.

[19] X Revenue and Usage Statistics (2026) - Business of Apps https://www.businessofapps.com/data/twitter-statistics/

[20] https://x.com/Waploadedblog

X should be aware of these issues through repeated right holder notifications. However, it has not taken the steps expected of a diligent operator to prevent or minimise copyright and VINL infringements on its platform. As a designated Very Large Online Platform under the DSA, X should be expected to treat copyright infringement and related illegal content as systemic risks requiring effective and proportionate mitigation measures. X should therefore remain listed on the EU Counterfeit and Piracy Watchlist.

Discord

Discord is a serious concern to the music industry as it is being used to set up online communities dedicated not only to discussing music, including specific artists and music content, but also to sharing or providing access to infringing music content, including pre-release music.

The ability to share files on the servers creates a significant issue for right holders, as users can easily upload infringing content and share links to infringing content hosted elsewhere, such as on cyberlockers. Users on a free subscription are offered the ability to join up to 100 servers and upload files up to 20mb (the typical song is about 5mb depending on the quality of the recording and the bitrate of the encoding).

Most notably and problematically for the music industry, Discord has become an underground marketplace for the distribution and crowd funding of stolen, unreleased or pre-release content, though so-called 'Group Buys'.[21] This is when a Discord server is used to conduct an auction to sell unreleased or pre-release content. Such 'Group Buy' servers are usually private, which means that they can be accessed by invitation only. Users within the server are invited to donate towards the Group Buy. Once the target has been reached, the track is shared to all users that contributed to the sale. Typically, the content is shared via a link to a cyberlocker, such as Pillowcase.su (as discussed above), where the infringing content is hosted and can be downloaded. Once the infringing content has been downloaded, it can be freely shared further.

In addition, over the past couple of years, we have seen a growing number of Discord servers dedicated to AI generated outputs and vocal clones. These servers typically assist and encourage users (including by providing 'how to' guides, links to illegal services such as stream ripping services, and ready-made AI voice models or vocal cloning bots) to make artist voice models and/or use artist voice models to produce outputs incorporating artist vocal clones. The creation of such vocal clone covers involves multiple acts of unauthorised reproduction, and the output can infringe both the copyrights in the original sound recording, as well as violate the personality rights of the individual whose voice has been cloned by the AI model.

Further, another concern for the music industry is that many third parties have created bots for use on the Discord platform, which enable users to listen to and interact with music

[21] A Group Buy through Discord is where a user sets up a private Discord server/channel for the purpose of the crowd funding and subsequent distribution of unreleased music content. The operator of the server/channel typically sets a target selling price and once that target has been met through user donations, the pre-release sound recording or group of sound recordings is distributed to all of the contributing users.

sourced from a third-party streaming platform (such as YouTube or Spotify, for example), whilst using the Discord service, in a manner comparable to a subscription-based licensed streaming service, but often in breach of the platforms terms and conditions and without relevant authorisation from, or remuneration to, the copyright owners. Not only do these bots source content from streaming platforms but they have also been created to help facilitate distribution of copyright content. These bots support crowdfunding communities know as 'Group Buys' where users can contribute financially towards unreleased material that is being sold within a Discord server. These bots have purposely been designed to assist the bad actors manage revenue received from other users.

Many of these third-party music streaming bots are themselves monetised via subscriptions, often using services such as Patreon as the paywall. Patreon is a subscription or membership-based platform that lets creators build income by offering exclusive content for communities. This type of funding allows the bad actors to profit but also monetise their creations outside of Discord.

Discord is an attractive platform for all this infringing activity due to a number of features, including the ability for users to set up private servers and the ability for operators of the server to remain anonymous. Discord's private servers are well suited in particular to 'Group Buys' as they allow users to engage other users anonymously, in a closed and unmonitored environment. In relation to bots, it is extremely easy for a user to create a bot and for users to add such third-party bots to their servers (including music bots allowing users to stream music without authorisation from the right holders). Discord also provides a searchable and categorised app directory for many thousands of third-party bots, including music streaming bots described above.

Why it should remain listed on the Watchlist

Although it is clear that the service is used in the ways described above, due to the structure of the site, including the availability of private servers, it is not easy for right holders to comprehensively search for infringements of their content on the service. Between August 2025 and July 2026, IFPI and national groups collectively reported over 12,000 infringing URLs. The scale of infringement on the service is likely to be much larger than has been detected to date. Discord should be required to take effective measures to ensure that the service is not used to infringe copyright, or be used in the facilitation of illegal acts, including without limitation, by expeditiously removing servers, channels and bots that are used to distribute music and other copyrighted content unlawfully, or to procure, assist or enable such activity to take place, and preventing those groups/channels and their operators from reappearing on the service.

Furthermore, from March 2024, Discord released an update whereby the display of Discord usernames would be changing. Users can now set non-unique display names with spaces, special characters and emojis. This allows a user to change their display names regularly. Although a username is required to be unique, how their display name appears in chats hinders investigations as become unrecognisable.[22]

[22] https://support.discord.com/hc/en-us/articles/12620128861463-New-Usernames-Display-Names#h_01GXPQAGG6W477HSC5SR053QG1

Telegram

Telegram is one of the largest online communications services in the world and a substantial proportion of its user base is located in Europe. Telegram began as a messaging application with privacy being a central feature. Secret chats, for example, are tied to individual devices and are not stored within Telegram's cloud infrastructure.

Now, Telegram is much more than a 1-2-1 messenger service as it offers features which are similar to those of social media networks with content/messages/posts being disseminated to groups and channels with an unlimited number of users. Given this, and the number of users of the platform, IFPI considers that Telegram should be designated as a Very Large Online Platform under the DSA.

Why it should remain on the Watchlist

Telegram continues to be used extensively for the unauthorised distribution of music through a variety of features available on the platform:

- **Channels:** These are tools for transmitting one-way messages/content to an unlimited number of subscribers. Channels can be used to push infringing music content to subscribers for download and/or streaming and typically include a search functionality which allows subscribers to easily locate music. A selected audio file can be streamed and downloaded.

- **Bots:** These are third-party applications which can be used as specialised search engines to locate music (e.g. a particular track by a given artist). The bot is an automated programme that responds to user commands. Telegram allows developers access to an API to create bots and the code for many bots is available on online software repositories such as Github. Bots that distribute infringing music can be easily located using a search engine or on social media.

- **Groups:** Content can also be shared between individuals within groups which can have up to 200,000 members.

Telegram is a platform for large scale content distribution. In a year, we reported 368,306 distinct URLs for infringing content. This includes 16,693 specifically for Taylor Swift content and 14,731 for Juice Wrld content. Telegram is also used amongst the pre-release community, with many channels dedicated to pre-release content sharing.

Music from Telegram can be saved to the user's device or streamed on the app, including for "background listening" when the app is closed.

Negative effects on the legitimate market

Unauthorised distribution of music on Telegram undermines the legitimate digital music market by offering features that compete with licensed download services and streaming platforms, without a licence. Music is distributed on a vast scale and secrecy means that right holders cannot identify and pursue operators of infringing channels and bots.

Telegram has been the subject of action:

- The Italian Federation of Newspaper Publishers applied to AGCOM in relation to channels that were illegally distributing unauthorised copies of newspaper publications. The prosecutor issued an emergency order requiring Telegram to shut down the infringing channels, failing which, AGCOM would require ISPs to block access to the Telegram service in Italy. Telegram subsequently shut down the relevant channels.[23]

- In 2021, the IP Court of Lisbon ordered Telegram to block access to 17 channels devoted to online piracy, with over ten million members combined in an action brought by Visapress[24] and GEDIPE[25] acting on behalf of publishers and the film industry respectively.[26]

- In 2022, the Delhi High Court granted interim relief to rights holder Doctutorials Edutech Pvt Ltd ordering Telegram to take down unauthorised copyright-protected material posted on channels. Telegram was also ordered to provide details of offending parties that it has available.[27]

- In 2024, a Spanish judge ordered the temporary block of Telegram following a complaint filed by several major media groups alleging that Telegram was hosting and distributing unauthorised copyright-protected content. ISPs were ordered to block Telegram whilst the claims were investigated. The block was however, quickly lifted following widespread complaints that it was disproportionate to block the entire service given the platform's widespread legitimate use.[28]

- In March 2026, India's Ministry of Information and Broadcasting directed Telegram to disable access to more than 3,000 channels identified as distributing pirated films, web series and audiobooks. The notice followed complaints from content owners and required the relevant channels to be removed or disabled within three hours. It was issued under the Information Technology Act 2000 and the Information Technology Rules 2021, with the Ministry warning that non-compliance could affect Telegram's safe harbour protection.[29]

IFPI's engagement with Telegram has resulted in improvements to the takedown process and infringing content is now removed in response to valid notices but large quantities of infringing material remain available on the service. Enforcement remains heavily dependent on right holders first identifying the infringement. Telegram also continues to provide features, including background listening, that allow users to consume infringing music in a

[23] Delibera n. 164/20/CONS
[24] Gestão de Conteúdos dos Médiato
[25] Associação para a Gestão de Direitos de Autor, Produtores e Editores
[26] Reference: 461343 Precautionary Procedure (CPC2013) No. 520/20.0YHLSB, Applicant: Visapress - Gestão de Conteúdos dos Media, Crl and Others, Defendant: Telegram Fz Llc, Date: 15-11-2021
[27] In the High Court of Delhi at New Delhi + CS(COMM) 60/2022 & I.A. No. 1338/2022 (O-39 R-1 & 2) Doctutorials Edutech Private Limited v Telegram FZ-LLC & ORS.
[28] High Court orders temporary suspension of Telegram's services in Spain | Reuters
[29] Govt orders Telegram to disable over 3,000 piracy channels in 3 hours | India News

manner comparable to licensed services. Further measures are therefore required, including stronger preventative controls, more effective action against repeat infringers and the introduction of robust know your customer procedures.

Vimeo

How it works

Vimeo was created in 2004 by Jack Lodwick and Zach Klein. In November 2025, Bending Spoons acquired Vimeo for USD 1.38 billion in cash. As a result, Vimeo Inc. was delisted but continues to exist as a privately held subsidiary within the Bending Spoons group. Vimeo is a video hosting and sharing platform that focuses on the delivery of high-definition video across a range of devices, deriving revenue by offering subscription plans to registered users. The platform focuses on original video content and offers its users access to tools for video creation, editing and broadcasting.

According to Similarweb, the site received over 645 million visits in the last 12 months globally (July 2025 to August 2026) with its top traffic coming from the USA, UK, Japan, Brazil, India, Canada, France, Spain, Germany and Australia.

In December 2024 Vimeo publicly announced that it had made changes to its service when accessed from the EU and the UK due to regulations targeting online platforms. As a result, Vimeo operates differently depending on whether the service is accessed from the EU and UK or outside of the EU.

Outside of the UK and EU, the platform continues to operate as a user-uploaded content service which engages in making available to the public music videos, including sound recordings, with a high degree of involvement by the service in the organisation and promotion of the content for profit making purposes. In spite of its involvement in copyright restricted acts, Vimeo has so far fallen short of its obligations to make best efforts to secure a license from copyright holders or to take effective steps to stop and prevent unlicensed music from being made available on its service.

Record labels have attempted to engage with Vimeo on numerous occasions in respect of the vast amount of infringing material hosted on the platform but have had no meaningful cooperation from the platform, particularly with preventing repeat infringements of notified content. The continued presence of vast amounts of infringing material on the platform, and minimal effort made by Vimeo to engage in discussions with right holders, or implement effective procedures to prohibit the uploading of infringing content, make it an ongoing piracy problem. This harms the ability of record labels to secure a return on their investment in artists which is crucial to their ability to invest in new artists. As a consequence, record labels initiated legal action against the service in Italy.

K) "Other" types of service – Intermediaries

Intermediaries play a crucial role in the fight against online piracy because they are used to commit copyright infringements and are often best placed to prevent it. This is true of all types of intermediary services including internet access providers, hosting service providers,

search engines, advertisers, domain registrars, domain registries, app stores and payment providers.

It is often very difficult, or even impossible, to identify the primary infringers as there are many ways in which operators of infringing services are hiding their identities. The situation is aggravated by the absence of an effective know your (business) customer (KYBC) obligations, particularly in relation to hosting providers and domain registrars and registries. In relation to domain registrars, there is a particular issue with domain privacy services, often offered by the same registrar which allow operators of pirate sites to remain anonymous. Even when the primary infringers can be identified, enforcement remains challenging because the infringers are often based outside of the EU.

The unavailability of remedies against the infringer puts the spotlight on intermediaries and right holders' ability to obtain injunctions against them, specifically on a no-fault basis. However, in most EU Member States, the system of intermediary injunctions is not effective enough to tackle the problem of online piracy.

These intermediaries should adopt meaningful measures to prevent copyright infringement occurring via their services, such as the adoption of effective repeat infringer and KYBC policies.

While the EU legislative framework, specifically IPRED provides for a good legal framework, the enforcement regime is inefficient because the EU norms have not been correctly implemented or are not correctly applied by national courts.

Njalla

Njalla is an anonymous intermediary for domain registration, hosting and VPS services. Its homepage notes that it is "considered the world's most notorious 'Privacy as a Service.'

Different to how other registrar services operate, rather than the customer owning the domain upon registration, Njalla owns the domain and grants the customer full control while shielding from public WHOIS lookups and potential disclosure requests. Additionally, Njalla operates as a proxy service for ICANN accredited registrars such as Tucows, buying domains on the customer's behalf to provide privacy.

Other services can also be acquired from Njalla if the domain has been registered using a different registrar, such as VPN and VPS services. The service has been specifically designed to provide enhanced privacy for customer details.

Njalla is supporting Anna's Archive, a shadow library referenced earlier in our submission, with two out of the three Anna's Archive domains using Njalla as the nameserver.

CloudFlare

Cloudflare is included again because its services are widely used by websites involved in copyright infringement. Cloudflare provides internet infrastructure services including CDN, reverse-proxy, DNS, security, caching and privacy services. As an intermediary between users

and websites, its services can materially affect both the identification of infringing services and the effectiveness of measures designed to prevent access to them.

Cloudflare operates one of the world's largest networks, spanning more than 335 cities in over 125 countries, directly connecting with approximately 13,000 networks and proxying around 20 percent of web traffic. Its scale, and the widespread use of its CDN, reverse-proxy, DNS and security services, make its role particularly significant in the online piracy ecosystem.

Where a website uses Cloudflare's reverse-proxy/CDN services, users generally connect to Cloudflare infrastructure rather than directly to the website's origin server. Public DNS and Network WHOIS information will therefore often identify a Cloudflare IP address rather than the underlying hosting provider or physical/jurisdictional location of the infringing service. While these services have legitimate security and performance purposes, they can also make enforcement significantly more difficult by obscuring the infrastructure used by infringing services.

Cloudflare has already been the subject of enforcement action in relation to piracy websites. In 2022 and 2023, the Court of Milan required Cloudflare to prevent access through its public DNS service to copyright-infringing BitTorrent sites and mirror sites that had been ordered blocked in Italy. More recently, in January 2026, AGCOM imposed a sanction of more than EUR 14 million on Cloudflare for failing to comply with an order under Italy's anti-piracy legislation requiring it to disable DNS resolution and routing to domains and IP addresses reported through the Piracy Shield system, or otherwise adopt measures necessary to prevent user access to unlawfully distributed content.

Cloudflare's Trusted Reporter programme gives certain right holder organisations, including IFPI, access to limited information, including some origin IP and hosting information. However, IFPI's experience is that the programme does not generally provide customer-identifying information, such as customer contact details, without legal process, such as a DMCA subpoena or court order. Disclosure of such information is therefore generally legally compelled rather than the result of a voluntary right holder-support mechanism.

IFPI welcomes Cloudflare's public statements that it has adopted a repeat-infringer policy, and its more recent transparency reporting showing increased action against copyright infringement involving content hosted directly on certain Cloudflare products, including termination of R2 services associated with more than 21,000 accounts in the first half of 2025. However, concerns remain as to how effectively and consistently notices relating to non-hosted services, including CDN, proxy and DNS services, result in meaningful action against customers repeatedly associated with copyright infringement. Greater transparency is required regarding the operation of Cloudflare's repeat-infringer policy across these services, together with clearer reporting to right holders on action taken following notifications.

Cloudflare should also implement a meaningful KYBC. Right holders often have to seek customer information through US legal proceedings, including under section 512(h) DMCA subpoenas, but the quality of information obtained can vary significantly. Cloudflare should verify customer information proportionately and refuse or discontinue services where customers do not provide accurate and verifiable identifying and contact information. Following credible notifications or other red flags, Cloudflare should review whether its

services are repeatedly being used for unlawful activity and take proportionate action, including termination where appropriate.

Cloudflare should take effective action where its services are used by customers whose activities have been established to infringe copyright. Where Cloudflare hosts or caches infringing content, it should disable access following valid notification. More broadly, its caching and availability services should not be provided in a manner that assists notorious piracy services to maintain availability following legitimate enforcement action.

Cloudflare should also ensure that its 1.1.1.1 public DNS resolver and WARP service do not undermine lawful website-blocking orders. DNS blocking is a principal method used by ISPs to implement such orders, and public DNS resolvers can provide users with a means of avoiding ISP-level DNS blocking. The Italian proceedings and AGCOM sanction demonstrate that Cloudflare-operated DNS and routing services can be required to support effective blocking measures. Cloudflare should maintain an effective mechanism for right holders and competent authorities to notify sites subject to valid blocking orders and ensure its services do not facilitate circumvention.

A further concern is Cloudflare's implementation of Encrypted Client Hello (ECH). ECH is a privacy-enhancing TLS extension that encrypts the Server Name Indication, meaning that intermediaries may see that a user is connecting to Cloudflare but not which Cloudflare-hosted website is being accessed. IFPI's technical analysis found that, in Cloudflare's implementation, the visible SNI may show a public-facing Cloudflare hostname rather than the actual target website. Cloudflare now enables ECH by default on Free zones, increasing its relevance to copyright enforcement.

ECH presents particular difficulties for SNI/hostname-based blocking because, where successfully negotiated, the ISP cannot identify the target hostname from the TLS ClientHello. While ECH does not make all blocking technically impossible, alternative measures such as DNS or IP blocking have important limitations. DNS blocking can be undermined where users use encrypted DNS technologies, while IP blocking is problematic in the context of large CDNs because many unrelated domains may share Cloudflare IP addresses, creating a risk of disproportionate collateral blocking. Cloudflare's own documentation recognises that ECH can affect domain-based network filtering and provides mechanisms for network administrators to disable ECH so that filtering can continue to function. This reinforces the concern that ECH can materially interfere with lawful blocking techniques that depend on visibility of the hostname.

l) Registrars/Registries

Domain registrars and registries play a crucial role in the online piracy eco-system, and they are uniquely positioned to take action to stop and prevent infringements. Examples of problematic ones include Namecheap, GoDaddy, PDR Ltd. d/b/a PublicDomainRegistry.com, Tucows, Tonic Registry and .Me Registry.

As previously highlighted, the main challenge that right holders still face is identifying the operators of websites which are dedicated to online piracy. It is often very difficult or impossible to identify who is operating a pirate domain, something that is exacerbated by the

misapplication of the GDPR and ICANN's excessive temporary policy with respect to access to WhoIs information. Since May 2018, ICANN and domain name registration services have prioritised their own risks under the GDPR over the interests of parties legitimately policing unlawful online activity by restricting access to WhoIs data, which effectively shields the operators of illegal websites and creates an environment that allows DNS abuse to flourish. Shortcomings in the existing legislative framework, such as the absence of a KYBC obligations on domain registrars and registries, allow unauthorised services to operate under the cloak of anonymity. It impedes legitimate enforcement of intellectual property rights by right holder groups such as IFPI against websites proliferating infringing content, causing substantial economic harm to right holders.

Domains are the gateway for public access to content online, including infringing content. DNS service providers, specifically domain registrars and registries, play a key role in online copyright infringement including by providing vital infrastructure that facilitates access to infringing services and content, and enabling operators to create recognisable 'brands' in connection with unlawful activities. In some cases, copycats use similar or alternative domains associated with notorious pirate 'brands' to attract traffic. They are also very well placed to help right holders tackle copyright infringement by implementing both preventative and reactive measures. Additionally, since domain registrars have a commercial relationship with registrants, they have access to certain information relating to their customers.

We have set out below some examples of the most problematic registrars and registries including Namecheap, Tucows and Tonic Registry which were included in the 2024 EU Counterfeit and Piracy Watchlist.

Namecheap

The US based registrar Namecheap is the domain registrar for over 290 problematic sites for the music industry including the problematic web download services trendybeatz.com and 9jaflaver.com. The registrar is also affiliated with long standing problematic cyberlockers such as nitroflare.com and ddownload.com. Following the launch of ICANN's RDRS in late November 2023, IFPI submitted a small number of requests via the system for disclosure of domain registrant details from Namecheap but they consistently refused our disclosure requests and ultimately, we stopped submitting requests.

According to Namecheap's Court Order and Subopena Policy[30] *Namecheap is a strong advocate for privacy. As such, and per our Privacy Policy, we cannot and will not share customer or account information except under limited circumstances when required by law or legal process properly served on Namecheap or one of our affiliates.*

Namecheap reserves the sole right to determine the laws that it is subject to and whether it has been properly served….. Namecheap is subject to US law and, in its sole discretion, determines whether it may be subject to other non-US jurisdictions.

[30] Namecheap.com - Legal - Namecheap Court Order & Subpoena Policy

Tucows

In contrast to Namecheap, the Canadian based registrar Tucows, does disclose domain registrant details on request but the details they disclose are very unhelpful as they are either incomplete, inaccurate or for a domain privacy service. From our experience, it is apparent that Tucows does not have an effective KYBC policy in place. They are currently the domain registrar for over 20 problematic domains for the music industry including meetdownload.com, megaup.net and m1xdrop.bz.

In April 2026, the Delhi High Court ordered the Department of Telecommunications and the Ministry of Electronics and Information Technology to take action against Tucows within two weeks following its refusal to comply with an order issued by the Delhi High Court in May 2025 in a case brought by the Premier League. Justice Gedela commented:

> *"This is unpalatable and unacceptable and appears to be clear defiance of the orders of this Court as also the previous orders passed by this Court, which were complied with after coercive measures were undertaken by this Court."*

From IFPI's experience, as was the case here, Tucows position is they will only comply with a court order issued by a court in Denmark, Canada, US and Germany. The Judge however, commented that *"It cannot be that the entity offers its goods and services in India and is able to appropriate financial gains and yet remain defiant and not submit to the jurisdiction of this Court."*

GoDaddy

US based registrar GoDaddy is one of the world's largest domain name registrars and continues to provide registration services to a range of websites engaged in or facilitating copyright infringement including sluhi.org, pagalworldmusic.com and playmp3song.com.

Due to its scale and market position, GoDaddy is particularly well placed to assist in efforts to combat online piracy. Pirate operators frequently utilise privacy and proxy services, making it difficult to identify those responsible for infringing activities. Despite the clear and repeated involvement of certain domains in copyright infringement, enforcement outcomes remain limited and infringing operators can often continue operating or rapidly migrate to alternative domains. Greater cooperation with right holders, improved verification of registrant information, and more robust enforcement of registrar terms of service would significantly enhance efforts to tackle online piracy.

Examples of other problematic domain registrars include Immaterialism, PDR Ltd. d/b/a PublicDomainRegistry.com, Name.com, Internet Domain Service BS Corp (IDS)/TLD Registrar Solutions Ltd /Central Nic. The holding company of IDS and TLD Registrar Solutions is the UK based company CentralNic cyberlocker.

Verisign

Verisign is the registry for the .com and the .net top-level domains which collectively account for a noticeable proportion of the domain name ecosystem. IFPI is currently aware of a

substantial number of notorious piracy services registered with Verisign including the following problematic sites: muzyet.com, muzrecord.com, paglaworldz.com, nitroflare.com, rilds.com, pagalworld4u.com, ddownload.com, Rapidgator.net, turbobit.net and jpfiles.net to name but a few. In light of Verisign's dominance in the registry ecosystem, they should play a greater role in ensuring the integrity of the domain name ecosystem and putting in place measures to prevent the misuse of .com and .net domains for systematic copyright infringement.

Public Interest Registry (PIR) (.org)

PIR is the registry operator for the .org top-level domain, one of the most widely recognised and trusted domain extensions globally. The .org domain was originally intended for organisations operating in the public interest and remains widely associated by internet users with legitimacy, trustworthiness and non-commercial activity. As the registry operator, PIR is responsible for maintaining the authoritative registry database for all .org domain names and occupies a critical position within the domain name ecosystem. The .org registry contains millions of active domain names and is relied upon by internet users throughout the world.

From a right holder perspective, PIR is of particular concern because a number of notorious piracy services have used, and continue to use, .org domain names to provide access to copyright-infringing content including hydr0.org and hiphopde.org. The credibility and consumer trust associated with the .org extension can assist operators of infringing services in attracting users and establishing an appearance of legitimacy. Pirate operators frequently exploit the reputation of established top-level domains to increase traffic and user confidence, notwithstanding the unlawful nature of the underlying activities.

PIR demonstrated that meaningful action is possible when, in January 2026, it suspended the .org domain name used by Anna's Archive following legal proceedings brought in the US by Spotify and RIAA. The suspension significantly disrupted access to the service and illustrated the important role that registry operators can play in combating large-scale online infringement.

However, the Anna's Archive matter also demonstrates a broader concern. Registry-level action typically occurs only after litigation, and evidential burdens have been satisfied. For many right holders, particularly in cross-border cases involving anonymous operators, obtaining such relief is costly, time-consuming and often impractical. As noted above registry operators are uniquely positioned to adopt proactive measures designed to improve the integrity of the domain name ecosystem, including robust KYBC requirements, effective responses to repeat infringers, and procedures to address domains supported by false, inaccurate or misleading registration information.

Given the scale and reputation of the .org namespace, PIR should play a greater role in ensuring that .org domains are not used to facilitate systematic copyright infringement. PIR should implement and enforce effective policies to identify and address repeat infringers, require accurate and verifiable registration information, and cooperate with legitimate rights holders seeking to tackle serious and large-scale abuses of the domain name system. Such measures would strengthen the integrity of the .org namespace while reducing its misuse by operators of notorious piracy services.

Tonic Registry

The .to country-code top-level domain ("ccTLD") for the Kingdom of Tonga is operated by TONIC Domains Inc. The .to namespace has, for many years, been disproportionately associated with copyright-infringing services, including stream-ripping sites, cyberlockers and other services dedicated to facilitating access to infringing content. As a result, the .to domain has become a recognised destination for operators seeking a stable and trusted domain extension through which to provide access to piracy services.

From a right holder perspective, the registry is of particular concern because a number of well-known piracy services have operated from .to domains. Examples include cyberlockers such as filestore.to and download services that have been repeatedly identified by right holders and, in some cases, have been the subject of blocking orders and other enforcement actions. Krakenaudio.to, which is associated with the problematic cyberlocker Krakenfiles.com has been criticised by OFCOM for hosting and making available CSAM content.[31] The continued use of .to domains by such services demonstrates the attractiveness of the namespace to operators engaged in large-scale copyright infringement.

The repeated appearance of .to domains in website blocking actions and piracy investigations demonstrates that registry operators are not merely passive technical actors. Registries occupy a strategic position within the domain name ecosystem and are uniquely placed to prevent the continued operation of domains used for systematic copyright infringement.

The registry has however, demonstrated as per PIR that it can take action when required to do so but only when subject to a court order. Following court proceedings in India, a number of .to domains associated with pirate streaming services were reportedly placed on client hold status, illustrating the important role that registry operators can play in preventing abuse of the domain name system. In July 2026, .to domains associated with major German-language piracy services, including s.to and bs.to, were suspended again following legal proceedings in India. The suspensions illustrate that registry-level action can have an immediate and significant disruptive effect on large-scale piracy services and demonstrate that the registry possesses the capability to take effective enforcement measures when it chooses to do so. However, the changes coincided with a restructuring where the Canadian domain name company Tucows took over the technical registry backend for .to domains.

m) Physical Piracy

Pinduoduo.com (PDD)

Pinduoduo (PDD) is an online shopping platform based in Shanghai, China. On this platform, sellers offer pirated music CDs, USB drives, and vinyl records. Users in mainland China can easily buy these pirated music products through PDD. Although it is not available in European markets, counterfeit products of European artists' music albums have been found on Pinduoduo, which impacts EU rights holders in Asian markets.

[31] https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/investigation-into-the-provider-of-krakenfiles-and-its-compliance-with-duties-to-protect-its-users-from-illegal-content

For its own business benefits, Pinduoduo has long allowed the sale of pirated music records. It ignores complaints from right holders and IFPI, and sets up very high barriers for filing complaints, in order to stop or slow down the removal of pirated CDs, USB drives, and vinyl records.

According to third-party data, PDD has about 900 million yearly active buyers in China, over ten million registered sellers, and handles more than 100 million packages per day on average.

With such a huge number of active users and sellers, combined with the platform's failure to comply with copyright law, PDD has become a major channel for selling pirated physical records. Many of the piracy cases that IFPI reports to China's copyright enforcement authorities each year—including both administrative penalty cases and criminal cases—involve sellers on PDD.

Shopee

Shopee is a Singapore-based B2C and C2C hybrid e-Commerce platform. It operates localised e-commerce platforms in Brazil, Indonesia, Malaysia, Singapore, Thailand, Vietnam, the Philippines, and Taiwan. It is one of Asia's largest online marketplaces, supported by integrated payments and cross-border logistics capabilities.

Shopee is one of the major e-commerce platforms where counterfeit music products are frequently available. Although Shopee is not available in European markets, counterfeit physical products of European artists' music albums have been found on the platform, which impacts and harms EU right holders in Asian markets.

Although Shopee has responded to right owners' complaints and acted against counterfeit listings and sellers in a timely manner, we have not seen sufficient measures by Shopee to prevent banned sellers from creating new accounts and continuing to sell counterfeit products on Shopee.

Shopee also imposes unreasonable requirements on right owners in some markets when they register a brand owner account on Shopee to report counterfeit goods, specifically requiring proof of copyright registration, which is not possible in most markets. Such requirements prevented right owners from being able to get access to Shopee's portal to report sales of counterfeit products.