IFPI Submission to the EU Counterfeit and Piracy Watchlist Consultation 2022: non-confidential version

14 February 2022

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

This submission identifies some of the major infringing online services that threaten legitimate digital trade in recorded music. We have listed infringing services with global audiences and also services which either defraud the industry in other ways or which do not apply measures expected from diligent operators or that reduce the risk of their services being used for copyright infringement purposes. This year we also want to raise the issue of "streaming manipulation" services which are a concern for the music industry in light of the potential market impact.

Some of the infringing services named in our submission were already listed in the EU Commission's 2020 edition, or even in the 2018 edition, of the Watchlist, such as Y2Mate/Youtubeconverter.io, Savefrom.net, Flvto.biz/2conv.com, Wi.to/Ddl.to (at its new domain name), Dbree.org, Rapidgator.net, 4shared.com, 1337x.to, rarbg.to, The Pirate Bay, Music-bazaar.com/Music-bazaar.mobi and Telegram. Unfortunately, most of them or their clones continue to operate. This submission discusses the factors that have led to this situation and offers suggestions for actions that could be taken by the EU to increase the effectiveness of the Watchlist from the perspective of copyright industries.

The nature of online music piracy necessitates not only increased international cooperation between law enforcement agencies and administrative and judicial bodies, but also access to meaningful information and evidence, legal remedies tailored to the online environment, including fast, flexible and catalogue-wide injunctions, with cross-border effects in the EU, and broader adoption of best practices by certain types of online intermediaries, especially in several jurisdictions named in this submission.

1. MUSIC PIRACY AND ITS RELEVANCE TO THE EU

Unlicensed distribution of our members' music reduces the economic incentives to invest in new music production – whether in foreign markets or in the EU. It damages the legitimate music market in the affected markets and has a negative impact on EU exports into third countries. Therefore, this submission covers both foreign-operated services undermining mostly EU markets as well as foreign-operated services undermining markets for EU music exports (including EU investment in music production abroad).

The EU is home to some of the most successful artists and music companies in the world. All these companies 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. European music companies invest in music production also in the third countries they operate in. Throughout the music ecosystem, record labels are the engines of the broader music sector[1] but their ability to continue investing in new talent is dependent on the ability to license their rights on fair economic terms, or to have unlicensed services closed down through legal actions where necessary.

2. ECONOMIC HARM

The various unlicensed services mentioned in this submission involve the unauthorised use of IFPI member companies' repertoire to make it available online on a global basis in violation of music producers' rights[2] enshrined in international treaties (WIPO Internet Treaties[3] and the TRIPS Agreement) and the domestic copyright legislation of many countries. Many of those services (or their predecessors), namely: Flvto.biz, 2conv.com, 4shared.com, Y2mate.com, 1337x.to, Savefrom.net, Snappea.com, Mega.nz, Dbr.org, Music-Bazaar.com and Rarbg.to have already been the subject of court judgments and other orders in various jurisdictions, but they continue to operate. Such unauthorised operation is economically damaging as it (i) diminishes the attractiveness of licensed music online[4]; (ii) reduces the revenue of licensed online music services thus undermining legitimate competition, and (iii) directly reduces the music sector's digital revenues which account for almost 70 percent (68.9 percent in 2020) of all music industry revenues.

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

[2] The rights of making available, communication to the public, reproduction, and protection against circumvention of technical protection measures that have been applied on behalf of right holders.

[3] Art.14 WPPT and Art. WCT

[4] IFPI 2019 Music Listening Report: 62 percent of those accessing content by unlicensed means would choose on-demand streaming to find and listen to music if copyright infringement was no longer an option.

The weight of academic research notes that piracy imposes significant economic harm on legitimate music revenues.[5] Calculating an estimate of the economic value of music piracy is difficult at present: previous research, in the era when physical sales were the predominant model of consumption, was based on a substitutional model that focused on the number of licensed downloads or discrete purchases which piracy prevented. Yet the recorded music industry is now dominated by streaming (62.1 percent share of global revenues[6]): music listeners tend not to buy individual tracks or albums as much but instead pay for a streaming subscription or listen to or watch individual streams on advertising-supported platforms.

IFPI's consumer research indicates that despite the wide availability of licensed content online through streaming, piracy still has a major impact upon the licensed streaming market. The most popular reasons for using piracy methods like stream ripping or cyberlockers are so that users can mimic the advantages of paid services (listening offline on a phone or portable speaker without interruption from adverts, having a permanent copy of music, using a method which is easy and convenient) – yet without having to pay. Thus, the economic harm from piracy is seen in fewer streaming subscriptions (and fewer advertising-supported streams) than in fewer purchases of downloads, CDs, or vinyl records. This presents a different research problem which previous methodologies are unable to address; it is a question yet to be thoroughly explored by academics or other researchers and industry, and no accepted methodology for the calculation of economic harm to the streaming business is currently available. As such, we will instead gauge the volume of piracy by providing estimates for the number of downloads occurring from infringing services to give a sense of the large scale of unlicensed activity which still takes place.

In addition to the difficulties in capturing the demand-denting effect of music piracy on the uptake of licensed music streaming offer, there are also difficulties with capturing the effect of pre-release piracy. Pre-release piracy relates to the distribution of music content that has not been commercially released. Such content is acquired by unauthorised means and as described below, there are business models (such as "group buys") which generate revenues from the sale of the stolen content and a premium can be charged for this exclusivity. Several services/platforms are involved in the initial distribution of pre-release content – these include messaging services, social media platforms and forums – such as Discord, Reddit, Leaked.cx and Telegram – where dedicated groups can be set up (often privately/by invitation only) for the purpose of promoting, funding the supply of, and providing access to leaked content. Expeditious action to close down these channels at an early stage is critical to containing the leak. The infringing content itself is usually stored on and shared via links to cyberlockers. At present, the cyberlockers that are active in the pre-release ecosystem include DDL/DDownload, Dbree, and Onlyfiles (other very popular cyberlockers that are involved in the distribution of pre-release content include Turbobit and Mega). The first three aforementioned cyberlockers do not respond to infringement notices and therefore have absolutely no regard for the use of their services for the distribution of infringing content.

[5] *Id. Citing* Smith M.D. and R. Telang (2012) "Assessing The Academic Literature Regarding the Impact of Media Piracy on Sales", Danaher B., M.D. Smith and R. Telang (2013) "Piracy and Copyright Enforcement Mechanisms", Innovation Policy and the Economy, Vol.14, pp. 25-61; and Danaher B., M. D. Smith and R. Telang (year ?) Advisory Committee on Enforcement, Tenth Session, Geneva, November 23 to 25, 2015, World Intellectual Property Organization.

[6] IFPI, 2021 Global Music Report.

They also operate anonymously which makes it very difficult to take any kind of direct action against them.

The leaked content is accessible to anyone with the relevant cyberlocker link and as a result there is limited opportunity for right holders to prevent onward distribution at this early stage. Once the leaked content is made available, it can then be distributed rapidly and widely on the internet on social media platforms such as Twitter, as well as other types of services such as linking and direct download sites. By this point, in the absence of any action beyond 'take down', right holders must expend substantial resource in seeking the removal of infringing content online as it appears, spreads, and reappears. The initial period following the official release of a new track/album represents a period of high demand. Every moment that the content is made available prior to release causes significant losses to our members, as well as the content creators. Although there are huge numbers of services that infringe our members' rights, due to the grave economic harm caused by pre-release piracy, the services mentioned above – Discord, Reddit, and Telegram – are considered enforcement priorities for the music industry and are a particular focus in this submission.

3. ONLINE SERVICES OFFERING ACCESS TO OR FACILITATING ACCESS TO COPYRIGHT PROTECTED CONTENT

a) 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.

We are currently tracking over 500 stream ripping sites. Some of the most popular and therefore, most damaging ones are set out below.

Trends in stream-ripping

IFPI's Music Consumer Study 2021, the largest music-focused consumer study worldwide found stream ripping to be the key music piracy threat. The study was conducted in 21 countries gathering the views of 43,000 respondents. The study found that 27 percent of respondents had used stream ripping sites as a way to listen to or obtain music and this figure rose to 35 percent amongst 16 to 24 year olds.

Search engines are the primary method by which users discover and find their way to stream ripping sites. Typically, over half of all visits to popular stream ripping sites occur after a search query. This high level of search engine activity distinguishes stream ripping from other piracy methods such as cyberlockers and BitTorrent indexing sites.

According to data from SimilarWeb, more than 95 percent of visits from search to stream ripping sites comes from Google. A delisting program has been in place since October 2019 and in addition, we are aware that, since December 2020, Google started demoting certain stream ripping sites as a way of tackling the trend amongst sites which were attempting to circumvent delisting. Whilst demotion appears to have had an impact with the small number of sites targeted seeing a decline in traffic, a further trend we have observed is for operators of stream ripping sites to run multiple such sites and have numerous domains registered so in the event of demotion or enforcement activities they have plenty of alternative domains waiting in the wings to which they can easily move[7].

A further trend we are seeing is for stream ripping sites to offer and promote apps on their sites for users to download. Y2mate.com, Snappea.com and Flvto.biz all offer apps on their sites for users to download. Snappea even has a QR code on its homepage for users to scan

[7] https://torrentfreak.com/theres-a-hidden-proxy-war-between-youtube-and-stream-rippers-201020/.

to download the app. By having the app on the site, rather than on for example, GooglePlay and the iOS App store, it ensures that the app remains available and cannot be subject to removal from the App stores following a complaint by a right holder. As an example of the scale involved, there have been more than 1.5 billion individual downloads of the SnapTube app alone during its lifetime. While it is not possible to know how many individual users this represents (the app has been available for a number of years), it demonstrates the scale of the problem involved.

1. Y2Mate.com and related sites

Over the last 12 months (January 2021 to December 2021) there have been over 1.5 billion visits to Y2mate globally with the traffic to the site increasing. To give a sense of scale, this is more internet traffic than the newspapers Le Monde (Lemonde.fr), or Le Figaro (lefigaro.fr). There were more than 905 million downloads of copyrighted music tracks from the site during 2021.

Users are able to convert and download either an audio-only MP3 file or the entire audio-visual work as an MP4 file through the site. There are three ways in which to do this; two begin with the user navigating to their desired YouTube video. The user then has two options that will both take them to the Y2mate.com homepage. Option one is for the user to add "pp" in front of the YouTube.com domain e.g. https://www.youtubepp.com/watch?v=VuNIsY6Jd. By doing so and then hitting 'enter' the user will be redirected to Y2mate.com, with the YouTube URL automatically copied and pasted into the conversion field on the site's homepage. From here, the conversion process continues as though the user had navigated to Y2mate.com themselves and manually copied and pasted the YouTube URL into the conversion field, and then pressed 'start'. The second way is for the user to copy and paste the YouTube URL into the conversion field on the site's homepage. The final way for the user to 'rip' content via the site is to use the search function on the site's homepage. The site offers a search function by keyword (e.g., artist or title name). The service will autocomplete to help the user locate the desired content.

The site promotes features on its homepage including "unlimited downloads and always free", "high-speed video converter", "no registration required", and "support downloading with all formats." The site also provides users with step-by-step instructions as to how to convert and download files.

Following music right holders' actions, Y2mate is currently subject to website blocking orders in Brazil, Ecuador, Peru, Italy and Spain.

Whilst the operator has voluntarily geo-blocked Y2mate.com from both the US and the UK, the operator has responded by registering the new domain YT1s.com which received over 774 million users between January 2021 to December 2021. Additionally, IFPI is aware that the operator is running other stream ripping sites including 9convert.com and Ytconv.cc. Moreover, voluntary measures are futile as they could be easily lifted by the operator at any time. Therefore, website blocking orders by European courts and authorities, remain the best available option for rights holders in tackling these sites.

2. Savefrom.net/ssyoutube.com/sfrom.net

Over the last 12 months (January 2021 to December 2021) there have been over 1.2 billion visits to Savefrom globally. To give a sense of scale, this is more internet traffic than the newspapers La Stampa (Lastampa.it), or Le Soir (lesoir.be).

The domain Savefrom.net, listed in the last edition of the EU Counterfeit and Piracy Watchlist, is also available from the domains ssyoutube.com and sfrom.net. Over the last 12 months (January 2021 to December 2021) there have been over 117 million visits to ssyoutube.com globally with traffic increasing. IFPI estimates more than 517 million downloads of copyrighted music tracks from the site during 2021. [8]

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 from? 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). More recently, in September 2021, the service similarly discontinued its operations in the UK. However, the service continues to operate in other territories outside of the USA and UK via the domains ssyoutube.com and sfrom.net.

Following music right holders' actions, Savefrom.net is now subject to a website blocking order in Spain. However, more blocking actions are needed to limit its availability 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.

3. Flvto.biz and 2conv.com

According to SImilarWeb, over the last 12 months (January 2021 to December 2021) there have been over 182 million visits to Flvto.biz globally and over 98 million visits to 2conv.com globally. Whilst not currently as popular as the two stream-ripping services mentioned above, these traffic volumes are still considerable. IFPI estimates more than 139 million downloads of copyrighted music tracks from the two sites during 2021.

Flvto.biz and 2conv are operated by the same individual in Russia and serve downloads of converted YouTube videos to users as digital audio files. All the user needs to do is to copy and paste a YouTube URL into a conversion bar on the sites' home pages and click on a

[8] Please see also page 3 above for an explanation of the methodology used.
[9] https://us.savefrom.net/

"convert to" button. These sites are dedicated to the mass-scale piracy of our members' copyrighted sound recordings.

These sites were listed in both the EU Counterfeit and Piracy Watchlist 2020 and the USTR Notorious Markets Report 2021. They have also been subject to civil litigation in the US. In October 2021, the U.S. District Court for the Eastern District of Virginia Court issued a default judgment in favour of the plaintiff record companies finding the operator liable for copyright infringement and the unlawful circumvention of a technological measure. In February 2022, the US District Court for the Eastern District of Virginia[10] ordered the operator to pay approximately USD 83 million in damages for copyright infringement and circumvention of TPMs.

Following music right holders' actions, the websites are currently blocked by ISPs in Australia, Brazil, Italy, Denmark, Ecuador, Russia, Spain and the UK. Flvto.biz is additionally blocked in Peru.

4. Snappea.com (including the app Snaptube)

Snappea.com is an example of how easily and quickly new damaging sites can emerge. In April 2021, the site received just over 32 million visits globally. By September 2021, Snappea.com generated 143 million visits globally (SimilarWeb). IFPI estimates more than 469 million downloads of copyrighted music tracks from the site during 2021.[11]

As at the time of writing, the functionality of Snappea's website varies depending on which country you access the service from and via which domain. The service is currently accessible via snappea.com, as well as via the Snaptube app. Further, the site is linked to snappae.com, which promotes the Snaptube app.

In addition to Snappea.com, there are similar looking and functioning domains (**s**snappea.com and the mirror site snappea.me). Although it is currently unclear if they are connected to Snappea.com, "Snappea" appears on the homepage.

When accessing Snappea.com from the US, users cannot stream or download any content from the site but are presented with a website promoting the app. Snappea.com is unavailable from the UK whereas snapp**ae**.com and **ss**nappea.com are available. When accessing Snappea.com via a VPN from China, the music industry's seventh largest music market and where the operators of the service seem to be based, users can both stream and download content. To obtain a copy of a YouTube video or 'rip' audio from the video, the user simply pastes a YouTube video URL into the converter bar or searches for the YouTube video in a search bar. The user can then choose a format (audio only or full video file) and clicks a download button. It appears that the service does not actually convert each URL on demand, instead the back-end domain is served by a CDN (Content delivery network). This CDN delivers a globally supplied network of proxy servers that cache content. Due to this,

[10] UMG Recordings, et al v Tofig Kurbanov, et al, Civil Action No.1:18-cv-957.
[11] Please see page 3 above for further explanation.

when a download is completed on the site, the content is cached, and the download link does not expire.

In December 2021, the São Paulo Criminal Court ordered ISPs to block access to Snappea and related domains for 180 days following an application filed by the Prosecutor's Office Anti-Organized Crime Group (GAECO), the Prosecutor's Office of the State of São Paulo (DEIC) and APDIF DO BRASIL (the recording industry Anti-Piracy association). In addition, as a result of the order, four of Snappea apps were removed from app stores in Brazil.

Snaptube app

The Snaptube application provides a very similar service as the Snappea website noted above, and allows the user to follow a stream ripping process, where they can obtain a downloadable permanent file stored on their device, even if the Snappea service is blocked at DNS level in a given territory. The Snaptube application works on the Android platform, although the application is not available via the Google Play App Store. The user can download it directly from Snaptube.com, Snappea.com, Snaptubeapp.com and Web.snappea.com, as well as other Android app stores such as EN.UPTOTOWN.COM, EN.APTOIDE.COM, and the HUAWEI App Gallery.

b) 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 they comply to some extend with 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 lockers 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 license.[12]

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 "Group Buys"**: Cyberlockers are frequently used to distribute snippets – or full versions – of leaked, pre-release content 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 often use encryption techniques for stored content, for example, using the Advanced Encyption 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

[12] 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.

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 remain private via a variety of privacy protection measures, such as masking registrant details with privacy protection services and making use of bullet-proof hosting providers that do not co-operate with efforts, by third-parties, for disclosure of client details.

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.

Ten years ago, the closure of MegaUpload, one of the most notorious cyberlockers, after 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. Yet in the last few years, cyberlockers have again increased in popularity: in Q4 2021, IFPI tracked 1.35 billion music-focused visits to cyberlockers, an increase of 5.2 percent compared to the same period in 2020.

While the figure for music-focused cyberlocker visits is lower than total global visits to the single most popular stream ripping site (Y2Mate), it is important to note that it reflects only those visits which seek pirated music; and also that while stream ripping sites tend to focus on downloads of individual music tracks, cyberlockers are also frequently used to download pirated albums as well as tracks. IFPI's experience in takedowns from lockers indicates that around half of cyberlocker music-focused visits are to obtain pirated music albums and half to obtain pirated tracks or singles. Taking into account that some attempted downloads from cyberlockers are unsuccessful (in part because IFPI manages a major notification and takedown operation aimed at removing content from cyberlockers), IFPI estimates that the equivalent of 6.14 billion pirated music tracks were successfully downloaded through cyberlockers in 2021 (around 472 million single tracks and around 5.67 million tracks contained on albums).

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. This role gives added importance to cyberlockers within the music piracy landscape.

6. Ddl.to

Why it should remain on the Watchlist

DDL.to continues to be a problematic cyberlocker for the music industry. The service was listed in the EU Counterfeit and Piracy Watchlist 2021, 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 pre-release content such as FRESHREMIX.RU, FAKAZAMUSIC.ORG, and HIPHOPDE.COM.

Additional Features and Functionality

The domain currently automatically redirects visitors to DDOWNLOAD.COM. It makes revenue via premium packages which provide features such as increased storage, quicker download speeds, and unlimited downloads. As of January 2022, the site also actively promotes discounted premium packages. Multiple file types can be uploaded onto DDOWNLOAD.COM.

Compliance and relevant actions taken

The site does not take any action in response to infringement notices. Please see also comments on page 9 above regarding the legal framework and the relevance of such actions.

Traffic

According to SimilarWeb, in the last 12 months (December 2020 to December 2021) DDL.TO has received over 11.04 million visits globally. The site receives over 70 percent of its traffic from Japan and over four percent of its traffic from Germany. Other countries in the EU, are listed within the top 20 countries that the site obtains traffic from. Although this traffic figure may not appear high in relative terms, the type of content being hosted; and the reputation of the locker as a platform where infringing content can be shared freely and anonymously – to the extent that significant traffic to it will be exclusively for this purpose – provides a greater indication of the domain's position as a major player in the online music piracy landscape.

7. Dbree.org

Why it should remain on the Watchlist

Description and Operator

DBREE.ORG is a 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 DBREE.ORG are frequently found on known leak sites and forums, including LEAKED.CX (of which it is a preferred/allowed hosting provider for posted content), LANABOARDS.COM, SHAREMANIA.US, and indirect music download sites such as ZIPTRAS.COM, and ITOPMUSICX.COM.

This cyberlocker makes available copyright protected content on the internet without authorisation from copyright holders and derives revenue from advertising. By using the domain DBREE.org it is capitalising on the popularity of another, unconnected cyberlocker, previously operated at the domain DBR.EE which was shut down in 2019, following coordinated action by IFPI, RIAA, and Music Canada on behalf of the music industry. DBREE.ORG is believed to be technically connected to a grouping of popular cyberlockers including NIPPYFILE.COM and NIPPYSPACE.COM, both of which have been subject to website blocking orders in France. Those involved in the distribution of pre-release music have gravitated towards DBREE.ORG as a key method of distribution thereby rendering this site a clear and present threat to the industry.

Additional Features and Functionality

The operator(s) of DBREE.ORG take several steps to try to hide their identities. For example, by using privacy protection services and making use of embedded redirect code in an effort to obfuscate where content is actually hosted. The domain is hosted by DDOS-GUARD LTD, a Russian-based bullet-proof hosting provider.

Compliance and relevant actions taken

The service is unresponsive to infringement notices, which means that leaked content shared on the service can proliferate unabated. Please see also comments on page 9 above regarding the legal framework and the relevance of such actions.

In November 2021, following an application by IFPI's Italian Anti-Piracy group FPM, the telecom regulator AGCOM ordered ISPs to block access to DBREE.ORG.

Traffic

According to SimilarWeb, in the last 12 months (December 2020 to December 2021) DBREE.ORG has received over 31.19 million visits globally. The site receives over 30 percent of its traffic from the USA and over five percent of its traffic from the United Kingdom. Other EU countries are listed within the top 20 countries sending traffic to the domain. Its mirror site, DBREE.ME, has received over 441,000 visits in the last 12 months and is most popular in The Netherlands – with over 45 percent of traffic – and the USA – with over 29 percent. Other EU countries are also listed within the top 20 countries sending traffic to the domain.

As with DDL.TO, although these traffic figure may not appear concerning, the type of content being hosted; and the reputation of the locker as a platform where infringing content can be shared freely and anonymously – to the extent that significant traffic to it will be exclusively for this purpose – provides a greater indication of the domain's position as a major player in the online music piracy landscape.

8. Mega.nz/.io

Why it should be listed on the Watchlist

Description and Operator

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. According to IFPI's Music Consumer Study 2021[13], MEGA was the most popular site used by respondents in the last month for downloading music, when presented with a selection of sites which included cyberlockers, stream rippers and BitTorrent sites.

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. Following a complaint from the film industry, US law enforcement initiated an action against the operators of cyberlocker Mega Upload in 2012. The action started with a raid on the operator's home in New Zealand, along with seizure of the site's servers and freezing of assets across multiple countries. Four individuals including Kim Dotcom were indicted for charges of copyright infringement, conspiracy and money laundering. Kim Dotcom continues to fight attempts to extradite him from New Zealand to face trial in the US. The US criminal investigation is still pending. Additionally, in 2014 the film and recorded music industries filed civil actions against Megaupload in the US and those cases are pending. 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.

Additional Features and Functionality

At the time of writing, the MEGA website claims to have over 245 million 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, last name and email address. 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.

[13] The study explored the ways people listened to, discovered, and engaged with music in twenty-one countries. It is the largest music-focused consumer study worldwide. In total, the survey gathered the views of 43,000 respondents.

MEGA allows users to create a Mega Cloud Storage, also known as Mega folders, in which uploads of up to 50 GB can be made without paying for a subscription. In addition, MEGA offers a referral program whereby existing users can earn 20 percent of the revenue from purchases of new users referred to MEGA. The scheme encourages existing users to invite new users, including by sharing content with them by invite, referral link or links to a chat. 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 400 GB and 16 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.

Compliance and relevant actions taken

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 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.

Traffic

According to SimilarWeb, in the last 12 months (December 2020 to December 2021) MEGA.NZ has received over 2.4 billion visits globally. The site receives over eight percent of its traffic from the USA and over five percent of its traffic from Spain. Other countries in the EU are listed within the top 20 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, more recently, MEGA.NZ automatically redirects users to MEGA.IO which has received over 89 million visits during the last 12 months and is most popular in the USA with over 9 percent and Italy with over four percent of traffic. Other countries in the EU are also listed within the top 20 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.

9. Onlyfiles.io

<u>Why it should be listed on the Watchlist</u>

Description and Operator

The site is an issue for the music industry as it makes available to the public pre-release content, often via links posted to prolific leak sites/forums including LEAKED.CX; LANABOARDS.COM and indirect music download sites such as BAZENATION.COM. It is also frequently seen in the dissemination of snippets and tracks sold/promoted in the course of Group Buys. Onlyfiles was also previously listed as one of the preferred file hosting services by LEAKED.CX

The domain's operator remains unknown.

Additional Features and Functionality

The website's functionality is very straightforward, and the site differs from other cyberlockers insofar as it actively encourages users to upload their music directly on the homepage without a requirement to register, log in or take any other action. File formats available for upload include MP3, MP4, WAV, OGG, AIFF, FLCE, and ZIP files.

Compliance and relevant actions taken

ONLYFILES.IO is non-compliant with infringement notices. Please see also comments on page 9 above regarding the legal framework and the relevance of such actions.

Traffic

According to Similar Web, in the last 12 months (December 2020 to December 2021) ONLYFILES.IO has received over two million visits. The site receives over 49 percent of its traffic from the USA and over two percent of its traffic from Italy. Other countries in the EU, are listed within the top 20 countries that the site obtains traffic from. The traffic numbers are not reflective of the issue which the domain causes; as the platform actively encourages individuals to share – and by extension source – pre-release content by whatever means, whether this be via hacking, theft etc.

10. Turbobit

<u>Why it should be listed on the Watchlist</u>

Description and Operator

TURBOBIT.SITE and TURBOBIT.ONLINE both redirect to TURBOBIT.NET.

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

Additional Features and Functionality

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-ons packages are available to purchase which allow the user to upload content anonymously.

Compliance and relevant actions taken

The domain is responsive to reports of infringements on its platform, however it should be required to take preventative measures such as content filters or warnings presented to the user when attempting to upload infringing content on the domain.

Traffic

According to Similar Web, in the last 12 months (December 2020 to December 2021) TURBOBIT.NET has received over 181 million visits.

The site receives over 14 percent of its traffic from Turkey and over 14 percent of its traffic from Japan. Other countries in the EU, are listed within the top 20 countries that the site obtains traffic from.

Other cyberlockers:

Rapidgator.net and **4shared.com,** which were listed in the 2020 Watchlist report, remain a problem for the music industry. That said, the cyberlockers listed above have been prioritised for entry on the Watchlist due to their role in the piracy ecosystem with respect to the distribution of pre-release content.

c) Other types of service offering access to or facilitating access to copyright protected content:

11. Audius

How it works

The AUDIUS platform describes itself as a decentralised "digital streaming service that connects fans directly with artists and exclusive new music"[14]. It comprises of a website and mobile application where users can upload music content for streaming, and download (where this functionality has been enabled by the uploader). Users can also create playlists

[14] https://docs.audius.org/welcome

and discover music on the service using a search function or browsing curated categories. The service positions itself as a platform to be used by creators of original music content to promote legitimate material, however a significant amount of content on the platform has been uploaded without the permission of the copyright holder.

The "Audius Token" ($AUDIO) is a form of cryptocurrency, and currently the platform's only source of revenue. It is claimed that users or operators of nodes (where content is stored) who stake the platforms' cryptocurrency, will receive a share of network fees, governance weight and other exclusive features.

Why it should be listed on the Watchlist

AUDIUS is a particular problem for the music industry as, despite being a user uploaded content platform at its core, it does not take measures to prevent infringing content from being made available on its service.

AUDIUS claims that it has no direct ability to remove any allegedly infringing content from the platform, or to cause any node operator to do the same (and rather, the operator of the applicable node should be entirely responsible for such content).[15] According to a page previously available on its website, AUDIUS purported that this is to protect against censorship.[16] However, it has been observed that the true purpose of this design is to seek to evade liability for copyright infringement, with the service being described as a "Copyright Nightmare"[17]. Further, a recent press article, states that AUDIUS is "plagued by piracy" and does not compensate right holders.[18]

AUDIUS has not consistently ensured the effective removal of all instances of notified infringing content accessible on the website and mobile application, nor does it appear to act against repeat infringers. AUDIUS is a platform whose primary focus is making available large amounts of music content and is well aware that there is a substantial amount of infringing content on the platform, including due to its receipt of infringement notices from right holders. Despite this, AUDIUS does not take any measures to prevent infringing content from being uploaded to the platform such audio content recognition technology or presenting copyright warnings to uploaders.

The service is growing in popularity and has been compared to the new generation Spotify or SoundCloud, which are licensed by right holders. In September 2021, AUDIUS announced that it had over six million monthly listeners.[19] According to Similar Web, in the last 12 months (December 2020 to December 2021) AUDIUS.CO has received over eight million visits globally. The site receives over 35 percent of its traffic from the USA and over three percent of its traffic

[15] https://audius.co/documents/TermsOfUse.pdf
[16] http://web.archive.org/web/20210415104734/https://help.audius.co/en/articles/3564542-how-does-audius-handle-piracy-and-unauthorized-uploading-of-copyrighted-material
[17] https://www.theverge.com/2019/10/9/20905384/audius-blockchain-music-streaming-service-copyright-infringement-piracy
[18] https://www.billboard.com/pro/audius-blockchain-streaming-service-piracy/
[19] https://twitter.com/audiusproject/status/1433248161443684356?lang=en-GB

from France. Other countries in the EU are listed within the top 20 countries that the site obtains traffic from.

d) BitTorrent Indexing sites

Trends

BitTorrent remains a major issue for music piracy: IFPI estimates that there were close to half a billion music-focused visits to BitTorrent sites in 2021 which led to over 2.75 billion equivalent track downloads, levels of which have been broadly stable over the last few years.

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, Rarbg, and ThePirateBay – all services listed in the 2020 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 stream ripping sites.

BitTorrent sites, including **1337x, Rarbg**, and **ThePirateBay**, all of which were included on the 2020 EU Counterfeit and Piracy Watchlist, 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.

e) Pay per download sites

Trends

There are a number of pay per download websites, including Music-bazaar.com and Music-bazaar.mobi (now: Songswave.com and Songswave.tel respectively), which are hosted from Ukraine (previously Russia). This category of sites remain popular with consumers and receive high levels of international traffic even though there are plenty of similar yet licensed download services available to users. In many cases the look and feel of the unlicensed pay per download sites is sufficiently professional to generate genuine confusion in consumers regarding the legitimacy of the service. The presence of well-known payment provider brands on the site (e.g. MasterCard, VISA l) further enhances the consumer deception potential of these unlicensed services.

12. Music-bazaar.com and Music-bazaar.mobi (now: Songswave.com and Songswave.tel)

As of mid-February 2022, IFPI has become aware that music-bazaar.com automatically redirects to songswave.com and music-bazaar.mobi automatically redirects to songswave.tel. Songswave.com and songswave.tel appear to be the same site with different domain

extensions. The two related services Music-bazaar.com and Music-bazaar.mobi[20] were listed in the 2020 EU Counterfeit and Piracy Watchlist.

Songswave.com has the same look and feel of Music-Bazaar.com and as per the previous domain engages in the unlicensed sale of singles and albums at a price which is significantly lower than if the user purchased the same single or album from a licensed service. The site describes itself as an online music store and allows users to "search for and download music in an easy and convenient way." Therefore, the site undermines the legitimate digital music market through direct competition with legitimate a la carte download services. Moreover, as the site pays no royalties to copyright owners, they have lower costs and are able to completely undercut legitimate licensed services and divert/reduce sales from licensed sites. Songswave has the look and feel of a legitimate licensed download service such as Amazon or iTunes for example as they have official album artwork and sell the latest releases as well popular older catalogue works. The fact that payment service providers such as Visa and MasterCard appear to provide services to the site deceives consumers into thinking these are legitimate sites.

In the same way as Music-bazaar, Songswave offers a wide range of international music repertoire with a particular focus on Italian, Greek, and Turkish artists but the site also sets out the 'Billboard – HOT 100 (World)', 'Top 100 iTunes US charts', 'Music Plus: Euro Airplay Chart (Europa). The site also has a "new releases" section and album of the day. The site claims to add "some 100 new albums" every day.

The sites are very easy and straightforward to use. Any type of user can use the site to browse content; however, in order to purchase and download music, the user is required to register and create an account. According to the 'help' section, the user adds money to their account using credit cards such as Visa or MasterCard or paymentcan be made for example, via bitcoin or bank transfer. A user then searches for the track or album they wish to purchase and then downloads their chosen track or album directly from the website. The price users pay normally varies depending upon the file size.

As noted above albums and tracks are available to purchase at significantly lower prices than their normal retail value . The site notes that the cost varies depending on the size of the song; "for a song of national catalogues is approximately 0.025 € for 1MB, and of world catalogue is approximately 0.02 € for 1 MB." The site also has a 'Free download' section from where users can download albums for free. Demos of all the songs on the site (lasting exactly one minute) are available without logging in to a user account. The purchased album will remain in the user's account for seven days and can be downloaded as many times as required by the user, on as many devices for no additional fee.

The domain songswave.com was registered on 28 January 2022 and the domain songswave.tel on 6 February 2022. As both domains are newly registered there is currently no traffic data available. However, over the last 12 months (January 2021 to December 2021), the predecessor site Music-Bazaar.com received over 1.3 million visits and received the highest volume of traffic from the US followed by Russia, Germany, Oman and Greece. The

[20] Music-Bazaar.mobi was a subdomain and a mobile version of the .com domain.

mobile version of the domain Music-bazaar.mobi received over 692,000 visits during this time. Traffic is not reflective of the issue which the domain causes because it enables users to purchase tracks at minimal price which in turn harms the rights holders.

Following court/administrative orders, Music-Bazaar.com is currently blocked by ISPs in Denmark, France, Greece, Russia and Spain.

f) Social media with infringing functionalities:

Trends

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 though 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.

IFPI's Music Consumer Study 2021, the largest music-focused consumer study worldwide, which was conducted in 21 countries gathering the views of 43,000 respondents, found that 14 percent of respondents used unlicensed social media platforms for music purposes. Of this, 23 percent said they uploaded and shared music, 21 percent sought unauthorised leaks of new music and 18 percent downloaded music.

Social media services which allow users to upload copyright infringing materials often claim – wrongly – protection from liability for copyright infringement by invoking "safe harbour" legislation, which was introduced in some countries to protect neutral internet intermediaries from spurious copyright claims. In Europe, however, the Directive on Copyright in the Digital Single Market Directive (DSM Directive) adopted in 2019 has brought important changes in relation to so-called "Online Content-Sharing Service Providers" (OCSSPs) clarifying that certain user-uploaded content services – "communicate to the public" or "make available to the public" – i.e. engage in copyright-restricted acts. Further, such services do not qualify for the "hosting service" liability limitation under Art. 14 of the EU E-Commerce Directive. This legislation is particularly relevant to many social media services with infringing functionalities (as well as cyberlockers, discussed further above) since it confirms that they have to modify their EU-facing operations and either get licensed for the music content made available on their platforms or ensure that no such unlicensed content is available there.

While Europe led the way in providing this clarification, it is evident that many services, notably some based in the US, often view their obligations as limited to compliance with US safe harbour laws and not the new EU standards of protection.

13. Twitter

How it works

Twitter is a widely used global social networking platform. According to Twitter's Global Impact Report, which was published in 2021, it reported 192 million Monetisable Daily Active Usage worldwide in Q4 2020. According to Twitter, it is a "*global platform for public self-expression and conversation in real time*." It allows people to "*consume, create, distribute and discover content and has democratized content creation and distribution*".

Its core service allows users to post "tweets" of up to 280 characters or "retweet" the posts of others. Tweets can include text, hosted content such as videos, and URLs that link to external sites. Twitter offers a highly organised service and search functionality, which all allow users easily to find and be served with content of interest.

The platform generates revenues, including from advertising of goods and services. Twitter's technology platform and information database enable them to provide highly sophisticated targeting capabilities for advertisers. Twitter's revenues for the 2020 fiscal year reportedly amounted to USD 3.72 billion.

Why it should be listed on the Watchlist

Twitter remains a significant concern to the music industry. Twitter stores and gives the public access to a large amount of copyright protected content and is a major platform for distributing infringing music content, both audio and video. This infringing music content includes both hosted content and links (including embedded links) to infringing music content hosted on external sites. Due to the social nature of Twitter, its volume of users and ease of access, the platform can be, and is used to share and distribute infringing material rapidly and on a massive scale, and the ability to re-tweet serves to amplify the damage that is caused by such infringements.

Many users make deliberate use of Twitter in relation to infringing activities precisely because of its large user base. Twitter is used to share links to websites or services from which infringing music content, including pre-release content, can be accessed either directly or indirectly (for example, users share links to cyberlockers such as MEGA (as discussed above) or to Discord channels (as discussed below).

Further, many infringing services, including ONLYFILES.IO[21], MEGA.NZ/IO[22], FLVTO.BIZ[23] and 2CONV.COM[24] (all discussed above) use Twitter 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 Twitter feed. These activities reach a large audience, thereby driving new users and more traffic to the infringing service.

Between May 2021 and Feb 2022, Twitter was notified by IFPI of over 366,000 infringements of music copyrights on its service, including over 25,000 pre-release music infringements.

[21] https://twitter.com/OnlyFiles
[22] https://twitter.com/MEGAprivacy
[23] https://twitter.com/flvto
[24] https://twitter.com/2conv

Further, Twitter still does not take steps to prevent future infringements of content that has been notified. Consequently, IFPI and its member companies spend a significant amount of time and resources identifying and notifying reappearances of the same content.

What is more, unlike any other platform, Twitter 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, Twitter 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.

Twitter is aware of the scale of infringements occurring on the platform as is evident from the number of copyright infringement notifications it has received. It has also more broadly been made aware of the music industry's grave concerns both by way of direct correspondence from recorded music industry trade organisations and via government-led roundtable discussions in the UK for example.

However, Twitter has not taken steps expected from a diligent operator to prevent or at least minimise the use of their platform for copyright infringement. Nor has it removed the perverse requirement that right holders pay Twitter for the possibility of identifying infringements of their rights on the platform at the scale required. To address the situation Twitter should be listed on the EU Counterfeit and Piracy Watchlist, which would incentivise them to do more to prevent infringements occurring and recurring on its platform.

14. Discord

How it works

Discord is a voice-over-IP (VoIP), instant messaging and digital distribution platform. It offers users access to a huge number of "servers", which further incorporate various topic-based "channels". Some of these are public, meaning they are accessible to all users of the service, whilst others are closed or private channels for a defined and controlled group of users. Users can communicate freely within a server with voice/video calls and text messaging and can exchange media, upload files and stream content. Discord has provided a free service to its users since its launch in 2015, but also offers a paid-for service comprising a two-tier subscription known as "Nitro", as well as purchasable features including, enhanced audio stream quality, greater upload file size and the ability to join a greater number of servers. The service also sells extra features ("Server Boosts") as well as merchandise. These are offered in three different packages, tailored towards the server size, community activity and cost. On average, a server booster is priced at USD 4.99 a month. Discord accepts major credit cards and PayPal.

As of 2021, Discord claims to have 150 million monthly active users, 19 million active servers per week and four billion minutes of server conversation daily[25]. Discord offers a web-based platform accessible via desktop browser as well as multiple versions of a free, standalone

[25] https://discord.com/company

application for mobile and desktop operating systems including Android, iOS, Linux, macOS and Windows.

Discord is a US registered company incorporated in Delaware. The company was originally incorporated on 22 March 2012. The company has branches in California and New Mexico, incorporated in May 2012 and January 2021 respectively. The company is headquartered at the California branch. The company was founded by Mr Jason Citron and Mr Stanislav Vishnevsky. Mr Citron holds the role of CEO, whilst Mr Stanislav holds the role of CTO.

As of January 2022, Discord's revenue model is based upon three sources, namely: (i) sale of premium subscription packages ("Nitro" – see above); (ii) sales of games (Discord partners with game developers who sell their games exclusively on their servers. Discord takes a ten percent commission on each sale); and (iii) Discord offers server "boosting" which, as described above, increases server functionality and performance.

Why it should be listed on the Watchlist

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 cyberlockers. Users on a free subscription are offered the ability to join up to 100 servers and upload files up to 8mb (the typical song is about 5mb depending on the quality of the recording and the bitrate of the encoding).

The Discord platform is an attractive platform for such infringing activity due to a number of features, including the ability for users to set up private servers, the ability for operators of the server to remain anonymous (a user can set up a server without requiring a verified email address or phone number) and the ease of using bots on the servers, which can perform tasks assigned to it by an admin user.

Most notably and problematically for the music industry, Discord has rapidly become an underground marketplace for the distribution and crowd funding of stolen, unreleased or pre-release content, though so-called 'Group Buys'[26]. This is where users use a Discord server to operate 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, often submitting smaller amounts of between USD 5 to USD 10 each. Once target has been reached, the track is shared to all users that contributed to the sale. Typically, this is via a link to a cyberlocker, such as ONLYFILES.IO (as discussed above) where the infringing content is hosted and can be downloaded. Once

[26] 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.

the infringing content has been downloaded, it can be freely shared further. Discord's provision of private servers allows users to engage quickly with other users in a closed and unmonitored environment, creating a platform where Group Buys can be easily organised on an anonymous basis.

Although it is clear that the service is used as described above, due to the structure of the site, including the availability of private servers, it is not easy for right holders to find infringements of their content on the service. Accordingly, 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.

Discord has been the subject of action, in respect of copyright infringement and malware, by several parties:

- In August 2021, YouTube sent a Cease-and-Desist order for "Violations of our Terms of Service including modifying the service and using it for commercial purposes" to the owners of a Discord bot named Groovy[27]. The bot could be added to a Discord server and stream music from YouTube, Spotify, SoundCloud and other services. The bot had been installed on over 16 million Discord servers. The owners of Groovy complied and shut down the service on 30 August 2021[28]. In an article concerning this case, Discord claimed that, "We take the rights of others seriously and require developers who create bots for Discord to do the same...If a bot running on Discord violates someone else's rights, that third party or Discord may take action."

- A report issued by Sophos News in July 2021 claimed Discord is now regularly used to host, distribute and control malware[29]. Their investigation into the use of TLS (Transport Layer Security) by malware, found that four percent of overall TLS protected malware downloads came from Discord. As Discord operates its own CDN, malware operators can upload malicious files to share with others. This included password hijacking software and leveraging Discord chat bots to obtain personal information.

According to Similar Web, in the last 12 months (January to December 2021), the site received 15.44 billion visits worldwide, with an estimated 22.96 percent of its traffic from the US. In December 2021 alone, the Discord App received 8,880,508 downloads on the Google Play Store and 12,318,182 on iOS.

15. Telegram

[27] https://uk.pcmag.com/social-media/135269/youtube-orders-shutdown-of-groovy-discord-music-bot
[28] https://www.theverge.com/2021/8/24/22640024/youtube-discord-groovy-music-bot-closure
[29] https://news.sophos.com/en-us/2021/07/22/malware-increasingly-targets-discord-for-abuse/

How it works

Telegram is a cloud-based mobile and desktop messaging application which is hugely popular globally. In January 2021, Telegram surpassed 500 million monthly active users with 21 percent of users coming from Europe.[30] The service was launched in 2013 by the founder of the Russian social media network VKontakte.[31] Telegram is currently incorporated in Dubai.

All Telegram messages and data are securely encrypted, with an additional layer of end-to-end encryption for "secret chats". Telegram has also deliberately structured itself to protect against disclosure of users' private conversations and personal data. For example, all secret chats are device-specific and are not part of the Telegram cloud. Telegram's business model is unclear and it currently appears that it is not operated for profit. It is believed that Telegram has not generated revenue since it was founded. The platform attempted to raise USD 1.7 billion via an Initial Coin Offering in 2018, however this fund-raising activity was halted by the US Securities and Exchange Commission in 2019, and was deemed as non-compliant with US securities legislation.[32] The founder claims to maintain the platform through the sale of his stake in the VK platform and via user donations, revenue data cannot be accessed from UAE National Economic Register. Future plans of the founders[33] indicate that the site will provide premium features, but users will still be able to maintain a free account, they have proposed introducing their own ad-platform

Why it should remain on the Watchlist

Telegram was listed on the 2020 EU Counterfeit and Piracy Watchlist. The platform continues to be used for the distribution of infringing music content, which can be done at a large scale via:

- 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. The content offered on a channel is curated by the operator and can be specific to a particular artist, genre, country or region. Channels typically include a search functionality which allows

[30] https://t.me/durov/147/

[31] vKontakte (VK) is a popular social networking service with a built-in music streaming functionality (now a licensed music service). In 2004, each of Universal Russia, Sony Russia and Warner Music UK issued proceedings in Russia (St Petersburg) against VK. In July 2015, VK entered into a licensing agreement with Sony Russia, and those proceedings were discontinued. Following the first instance and subsequent appeal decisions, VK entered into licensing arrangements with Warner and Universal thereby concluding the legal actions. Although the music service is now licensed, vKontake has continued to be a problem for other industries and was listed on the 2020 EU Counterfeit and Piracy Watchlist.

[32] SEC Press Release: SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering https://www.sec.gov/news/press-release/2019-212#:~:text=SEC%20Halts%20Alleged%20%241.7%20Billion%20Unregistered%20Digital%20Token%20Offering,-FOR%20IMMEDIATE%20RELEASE&text=%E2%80%9COur%20emergency%20action%20today%20is,the%20SEC's%20Division%20of%20Enforcement.

[33] 26/01/2021 - https://www.feedough.com/how-telegram-works-makes-money/ - 02/02/21 https://whatisthebusinessmodelof.com/business-models/telegram-business-model/

subscribers to easily locate content and/or include a browsable menu of all available content, including music content, news publications, films and television programmes. A selected audio file can be streamed and downloaded. Channels can be private which only allows subscribers that are added by the operator or receive an invitation to join or public which means they can be joined by any Telegram users. It is not difficult to find infringing Telegram channels offering music content using external search engines.

- Bots: These are third-party applications that operate within Telegram which can be used as specialised search engines to locate specific music content (e.g., a particular track by a given artist). Unlike a channel, where content is being shared by the operator, the bot is an automated programme that responds to user commands. For example, there are bots that feature commands that allow users to search by song title or artist name and will deliver the search results comprising of available audio files which the user can stream, permanently download, and share with other Telegram users. Telegram allows developers access to an API to create bots and the code for many bots are available on online software repositories such as Github. Bots that distribute infringing music and other copyrighted content can also 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. For example, we have witnessed the distribution of 2,663 audio files on a channel with 26,918 members[34], the distribution of 400 audio files on a channel with 75,975 members[35], and the distribution of 846 audio files on a channel with 18,936 members[36]. There are also so-called "hub" channels dedicated to music piracy which provide links to hundreds of other channels which make infringing content available.

Music content that is downloaded from Telegram can be saved locally to the user's device and played back including when offline, using the default media player or from within the application itself. Music content can be streamed within the application, including for "background listening" when the application itself is closed.

Negative effects on the legitimate market

The use of Telegram for the unauthorised distribution of music content undermines the legitimate digital music market by offering features that directly compete with licensed download services and streaming platforms, without paying anything to right holders. Due to the wide user base, music content can be distributed on a vast scale; the true scale is unknown due to the existence of private groups and channels. Further, Telegram's stance on secrecy means that right holders face challenges identifying and pursuing directly the operators of infringing channels and bots and users that share content via groups.

[34] https://t.me/rj1music
[35] https://t.me/samburiatko
[36] https://t.me/InfoTrapMusic

Telegram has been the subject of action in respect of copyright infringement:

- The Italian Federation of Newspaper Publishers (FIEG) filed an application with AGCOM in relation to Telegram channels that were illegally distributing unauthorised copies of newspaper publications. Following the complaint, an Italian prosecutor issued an emergency order in April 2020 requiring Telegram to shut down the infringing channels, failing which, AGCOM would require ISPs to block access to the entire Telegram service in Italy. Telegram subsequently shut down the relevant channels.[37]

- In November 2021, in proceedings for injunctive relief, 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[38] and GEDIPE[39] acting on behalf of publishers and the film industry respectively.[40]

- In January 2022, in proceedings for an interim order, 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.[41]

Following intensive direct outreach to Telegram by IFPI, the service has started to remove infringing content, channels or bots following a takedown request. While this process appears to be working, it barely tackles the problem given the large amount of infringing content remaining on the platform, including via bots, and because of right holders inability to find the infringing content in the first place. Telegram also continues to offer a background listening function which allows users to listen to infringing music outside of the Telegram app. Telegram should take effective measures to ensure that the platform is not used to infringe copyright, including more meaningful and proactive measures to stop and prevent copyright infringements via channels, groups and bots, implementation of effective repeat infringer and know your customer policies.

16. Vimeo

[37] *Delibera n. 164/20/CONS*
https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5lVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5lVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5lVOIXoE_assetEntryId=18496688&_101_INSTANCE_FnOw5lVOIXoE_type=document
Resolution n. 164/20/CONS

[38] Gestão de Conteúdos dos Média

[39] Associação para a Gestão de Direitos de Autor, Produtores e Editores

[40] *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

[41] *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.*

How it works

Vimeo was created in 2004 by Jack Lodwick and Zach Klein. Vimeo is a US-based 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. As of 2021, the site has 200 million users (being individuals, professionals, teams and organisations)[42] and around 1.6 million subscribers. Vimeo is available online and via a mobile application, and it provides its services in a number of languages including German, French, Spanish and Portuguese.

According to SimilarWeb[43] the site received 85.5 million visits from October to December 2021, with its top traffic coming from the USA, UK, Canada, France, and Germany.

Why it should be listed on the Watchlist

Vimeo is a very large user-uploaded content service which engages in the making available of 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 has had no meaningful cooperation from the platform, in particular when it comes to 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 rights holders, or implement effective procedures to prohibit the uploading of infringing content, make it a large, 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. Lawsuits against Vimeo are pending in Italy, including by the company RTI with the service having been ordered to pay EUR 8.5 million damages to the plaintiff for the making available of copyright infringing content (the decision is under appeal).[i]

17. Reddit

How it works

Reddit is a combination of a social news website – meaning that it features user-posted stories which are ranked based on popularity – and a social news aggregation site – meaning that it collects data from various social media sources to store them in a single display and web rating/discussion site. Posts are uploaded within communities, also known as subreddits,

[42] https://twitter.com/Vimeo/status/1397200988927315970

which is similar to a forum. An extensive number of communities exist within the platform. Subreddits can be public, restricted or private.

Reddit has a desktop site and applications for all major mobile and desktop computer operating systems, these include Android, IOS, and Windows. The platform also has a "lite" version of its app.

Reddit makes revenue via a premium service, which offers the user a variety of features such as ad-free browsing, Reddit coins, exclusive avatar gear and premium awards. The platform makes revenue via the sale of Reddit coins which are popular on the platform for user engagement reasonings.

The platform also makes revenue from advertising. Businesses can advertise on the site via advertisement accounts. According to Reddit COO Jen Wong, in 2019, the platform had an ad revenue of USD 100 million[44].

Why it should be listed on the Watchlist

There are currently over 2.8 million subreddits within the platform, and the site attracts a large audience (see below).

It is possible to upload several types of content on the platform including images and videos (.MP4 and .MOV formats). Although it does not permit uploads of MP3 files, Reddit is used for sharing links to infringing music content hosted on other platforms, including leaked, pre-release content. The structure of the platform makes it more challenging generally to find infringements at scale. However, we have detected many instances of pre-release content distributed across the platform, including on leak-specific subreddits. REDDIT is used in combination with other services such as Discord and Twitter to promote the distribution of pre-release content.

Although Reddit removes notified infringements and appears to implement a repeat infringer policy, the responsibility for monitoring the platform for unlicenced music content rests entirely with the copyright owner. As noted above, this is a burdensome process and there appears to be no proactive effort made by the organisation to reduce this burden. Reddit needs to take further steps to identify and address the illegal sharing of content, especially pre-release content, on the platform.

According to Reddit, the platform has over 430 million monthly active users worldwide, and 52 million daily active users. Reddit currently holds an Alexa ranking of No. six in the United Kingdom and No. 20 globally.

According to Similar Web, in the last 12 months (January to December 2021), the site received 21.71 billion visits worldwide, with over 48 percent of its traffic from the US and over seven percent of its traffic from the United Kingdom. Other countries in the EU, are also listed within the top 20 countries that the site obtains traffic from.

[44] December 2020 - https://www.wsj.com/articles/reddit-claims-52-million-daily-users-revealing-a-key-figure-for-social-media-platforms-11606822200

The Reddit app has had over 50.000.000 installs on Google Play and is ranked as No. two for News apps on The App Store.

"Other" types of service – Intermediaries

Intermediaries play a crucial role in the fight against online piracy because they are used to commit copyright infringement and are often best placed to prevent it. This is true of all types of intermediary service including internet access providers, hosting service providers, search engines, advertisers, domain registrars, domain registries, app stores and payment providers. These intermediaries should adopt meaningful measures to prevent copyright infringement occurring via their services, such as the adoption of effective repeat infringer and "know your customer" policies.

The music industry has concerns with several individual intermediaries, but primarily around certain domain registrars and registries (e.g., .to, Njala); domain privacy protection services (e.g., Internet Domain Services BS Corp, Domains By Proxy, LLC), and so-called bullet proof ISPs (e.g. Ecatel, Flocinet) which support various types of criminality through considerable leniency in respect of the kind of material they permit to be uploaded and distributed via their server networks. These hosts/bulletproof ISPs do not respond to notices of infringement or warning letters informing them that they are hosting and supporting known infringing sites. There are also increasing concerns in connection with piracy via mobile 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.

Several intermediaries have been named by IFPI in past submissions and we continue to have concerns about the services specifically mentioned. The focus of this year's submission is CloudFlare given its involvement in a high number of the music industry's priority sites.

18. CloudFlare

Many websites use Content Delivery Network (CDN)[45] and Domain Name Server (DNS) services. CloudFlare is an US based company that claims to serve data from 250 cities in over 100 countries. To give an indication of scale regarding the proportion of infringing domains using Cloudflare: CloudFlare provides a CDN service to seven (9 including mirror sites) of the

[45] A CDN is a system of distributed servers that improves the efficiency of the delivery of internet content to end users. The CDN works by delivering content from servers that are geographically closer to areas of higher user demand. CDNs typically achieve this by maintaining servers in data centres around the world. They replicate the website's content on each of the servers, so that the content can be downloaded from the place which is closest to the user, rather than having to deliver it from a central point, which may be a long way from where the user is physically located. The benefits to website operators of using a CDN include: (i) increased content delivery speed; (ii) ability to cope with a high level of web traffic that may overload the servers of the client website; and (iii) caching static content so sites may remain active even if a client website's server goes down. CDNs can also often offer benefits to website operators for dealing with network security threats such as hacking, DDoS attacks or viruses. Once a threat has been detected at one location in the CDN network, a solution or fix can be found to deal with it at the point where it was located, and then disseminated throughout the CDN network, thereby making that network more secure for all users.

infringing services named in this year's submission alone. This is a mere snapshot of the number of infringing services to which CloudFlare is providing services.

A consequence of using a CDN such as CloudFlare, is that right holders cannot determine the original IP address of the website that is responsible for delivering the content without requesting such details from CloudFlare. The directory will instead list the IP address of the server within the CDN from which the content is delivered. Therefore, it is not possible to discover from Network WHOIS the true location of the server(s) hosting the site. Services such as CloudFlare therefore provide anonymity to the owners and/or operators of the websites that use its services. This feature is particularly desirable for the operators of pirate websites, and others engaged in unlawful activity.

Why it should be included on the Watchlist

Whilst CloudFlare advised the European Commission that it offers the status of "trusted flagger" to some stakeholders including IFPI, such status only provides IFPI with access to limited information and amounts to nothing more than what right holders would normally be able to obtain, were the infringing services using the services of "traditional" access and or traditional DNS resolution services and the rights holder carried out a WhoIs LookUp on the IP address. Where IFPI needs to obtain the customer's contact information, CloudFlare will only disclose these details following a subpoena or court order – i.e. these disclosures are mandated by law and are not an example of the service's goodwill or a policy or measures intended to assist IP rights holders

Furthermore, notices or requests for information under the "trusted flagger" program should result in meaningful action vis-à-vis the customer. The program needs to feed into a repeat infringer policy, yet in the case of CloudFlare, there is no evidence that it does. CloudFlare should inform the right holder in respect of action taken against the site e.g., whether CloudFlare has suspended its services to the site.

CloudFlare should also implement a meaningful know your customer policy. Right holders are often required to seek additional information via the courts in the US, using the procedure provided under Section 512(h)(2) of the DMCA. However, the quality of information obtained varies significantly. It would appear that CloudFlare does not sufficiently verify information received from their customers, i.e., they do not operate a meaningful "know your customer" policy. CloudFlare should exercise due diligence in confirming who its customers are and establishing their proposed and actual activities. Currently, to our knowledge, CloudFlare has no process in place for verifying their customers' true identities. CloudFlare should refuse to provide services to customers who fail to provide accurate contact information. CloudFlare should also obtain details about the activities that the customers are planning to undertake. It should not provide services to customers that engage in illegal activities or violate CloudFlare's policies, and it should conduct further checks with respect to activities that fall under particularly risky categories.

Following notifications or other "red flags", CloudFlare should undertake periodic audits of customers to assess if they are engaging in unlawful or infringing behaviour and terminate services to customers when such unlawful or infringing behaviour is apparent.

CloudFlare should stop providing any of its services to customers whose account has been found to be infringing copyright. Where CloudFlare is providing CDN services, or when it is caching or hosting content, or linking to content, it should disable access to the infringing links and content for which it has been notified. The "Always Online Service" which allows sites to keep their pages online even when their server goes offline should not be available to notorious pirate websites.

In April 2018, CloudFlare launched their 1.1.1.1. app which is a public DNS resolver and allows users to access websites even if the domain name of that website has been blocked by ISPs, thus rendering sites blocked at DNS level only ineffective. The service has much broader repercussions than just the facilitation of copyright infringements, e.g., in relation to users' safety, malware, criminal activities in general. In September 2019, CloudFlare launched WARP and WARP+, a mobile app which according to CloudFlare uses their global network to secure the user's phone's Internet traffic i.e., WARP is a paid VPN service. Users who have installed the 1.1.1.1 app can enable WARP via the app on their device.

CloudFlare should make sure that its services do not undermine the effectiveness of site blocking orders and should implement a procedure whereby right holders can submit websites subject to website blocking orders and stop users from accessing these sites via the 1.1.1.1 app.

Litigation against CloudFlare

CloudFlare has found itself the subject of litigation in a number of countries, including multiple cases in Italy as set out below, a case in Germany, details set out below, numerous cases in the US[46] and most recently in Japan.

In Asia, IFPI is aware that four Manga publishers have filed an action with the Tokyo District Court seeking an injunction and damages against CloudFlare for copyright infringement[47].

[46] Examples of litigation in the US include: *American Chemical Society v Sci-Hub et al* – Case 1:17-cv-00726-LMB-JFA - In November 2017, in a case brought by American Chemical Society against Sci-Hub a permanent injunction requiring third party services, including domain registries, hosting companies and search engines, to stop providing access to the site was granted. In February 2018, Cloudflare terminated service to several domain names of Sci-Hub after notice of these proceedings. (cdn.arstechnica.net/wp-content/uploads/2017/11/schihubenjoin.pdf)
Elsevier Inc. v Library Genesis Project, Elbakyan et al – Case 1:15-cv-04282-RWS – In October 2016, a New York court ordered[46] Cloudflare to identify the operators of Libgen and Bookfi, as part of wider proceedings[46] brought by academic publisher Reed Elsevier against the two sites and Sci-Hub. Elsevier had previously attempted to obtain information through the "trusted notifier" programme, but because the sites were no longer active on its network, CloudFlare had argued that it could not share this information. This led to Elsevier filing a request at court in September 2016, explaining that a discovery subpoena was the only option to identify the defendants[46]. The court was satisfied that the websites were engaging in copyright infringing activities and that a subpoena was warranted[46]. It is not apparent whether relevant information was handed over by Cloudflare, particularly given that the two sites in question were no longer using Cloudflare's service when the request was granted.(torrentfreak.com/court-orders-cloudflare-to-identify-pirate-site-operators-161028/; torrentfreak.com/sci-hub-ordered-to-pay-15-million-in-piracy-damages-170623/; and torrentfreak.com/elsevier-wants-cloudflare-to-expose-pirate-sites-160917/)

[47] https://torrentfreak.com/manga-publishers-lawsuit-cloudflare-fails-to-terminate-pirates-or-verify-identities-220202/

In the EU, in February 2021, the Milan Court issued two decisions on appeal in urgent proceedings against CloudFlare. In both cases the Court confirmed prior orders issued in 2020 under which CloudFlare was under the duty to block the provision of services to illegal IPTVs, regardless of the qualification of said services as hosting, caching or other. The panel of judges stated that it is the right of the injured party to "obtain protection, both as a matter of urgency and in merit proceedings, against all those who contribute to the violation of the rights of others, even if the portion of conduct individually implemented does not constitute as itself an imputable violation of copyright". The Court found the argument put forward by CloudFlare that the termination of its services would not lead to the disappearance of the pirate sites to be irrelevant. The Court also dismissed CloudFlare's argument that it does not provide hosting services but merely passes on bits and bytes finding that CloudFlare contributes to the infringements of its customer by optimising and facilitating the site's availability. "It is in fact adequately confirmed that CloudFlare carries out support and optimisation activities to showcase sites, which allow the visibility and advertising of illegal services".

In earlier litigation, in January 2020, IFPI's national group in Germany, BVMI, was successful in obtaining a preliminary judgment against CloudFlare requiring it to stop making an album available to the public by providing services to the domain of a popular infringing site DDL-music. Consequently, CloudFlare blocked access to DDL-music. Both CloudFlare and Universal Music GmbH have appealed the decision. The decision was confirmed by the Higher Regional Court of Cologne in October 2020 which found that CloudFlare was unable to benefit from the internet access provider liability privilege because of the contractual relationship between CloudFlare and the website operator, and because CloudFlare had intervened in the data transfers in question. This meant that CloudFlare was not operating as a mere conduit and was also not covered by the caching privilege. As such, CloudFlare was found to have causally contributed to the infringement and therefore assumed responsibility as a 'storer' under German law. A DNS block was therefore required. Further, CloudFlare's arguments failed that it's making available of access to the DDL-Music domain was independent of use of its DNS resolver; that the preliminary injunction which required blocking of the entire domain was 'over-blocking' because it would apply worldwide; and that the blocking would be ineffective because the domain could still be accessed without using the CloudFlare DNS service. CloudFlare was found to have acted in bad faith, because it received notification of the infringements but took no action for eight months. As a storer, CloudFlare was under an obligation to review and block the domain as soon as the concrete copyright violation was pointed out.

On 24 June 2019, the Court of Rome issued a preliminary decision against CloudFlare which confirmed an earlier ruling in proceedings brought by Mediaset/RTI.[48] CloudFlare was

[48] CloudFlare Inc. and Reti Televisive Italiane s.p.a. (RTI) R.G.26942/2019. The court confirmed that the E-Commerce Directive and implementing Italian legislation did apply in respect of CloudFlare. It went on to describe CloudFlare's activities, and to determine that some of them qualify as hosting services. The Court found CloudFlare to not only be caching but also hosting, and subject to EU and Italian law regarding the liability exemptions for hosting provider services. Thus, it could only be protected against liability if it did not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or

amongst other measures ordered to: cease provision of services to certain pirate sites which allowed unauthorised access to Mediaset audiovisual works; provide a complete set of data to RTI/Mediaset identifying hosting providers and operators of the sites; and pay RTI EUR 1,000 for each day that the order is found to have been breached.

"Other Types of Services": Justanotherpanel.com

How it works

JUSTANOTHERPANEL.COM (JAP) is a Russian-based so called "streaming manipulation" service. Streaming manipulation involves the creation of artificial 'plays' on digital music streaming services ("DSPs"), such as Deezer, Spotify, SoundCloud and YouTube for example. Stream manipulation involves the artificial creation, by human or non-human means, of online or offline plays on audio and audio-visual streaming services i.e., where those plays do not represent genuine listening. Streaming manipulation may be undertaken in respect of individual or groups of recordings to artificially improve chart positioning, increase market share, increase royalty payments, or for other dishonest purposes. It is a form of fraud and it does not represent actual listening or genuine fan engagement activity. As such, it must be distinguished from marketing or promotional campaigns which encourage consumers to engage in sessions of genuine listening to particular artists or recordings.

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. There are two tiers of streaming manipulation services, consumer-facing sites (B2C) and larger wholesale suppliers (B2B).

JAP offers users the opportunity to purchase manipulation B2C services for a wide range of social media platforms such as Instagram, Facebook and Twitter as well as music-specific manipulation services on Spotify, Soundcloud, Apple Music, Amazon Music, Tidal and YouTube, with various packages available for purchase.

Further, JAP – through a connected site - also offers users the ability to buy their own 'panel' from which to start reselling streaming manipulation services to consumers. This is a wholesale B2B 'off-the-shelf' manipulation service available for various music services and appears to be part of a network of streaming manipulation services. Users are directed from JAP to a sister site to create this panel. Such a program incentivises other sites/individuals to 'resell' its streaming manipulation services.

circumstances from which the illegal activity or information is apparent; or if upon obtaining such knowledge or awareness acts expeditiously to remove or disable access to the information. The court went on to note that the deliberate continuation of the provision of services through which illegal activities are carried out, despite knowledge of such activities, can constitute collaboration with those engaged in illegal activities. As a result, and according to Recital 44 of the E-Commerce Directive, CloudFlare could not benefit from the E-Commerce safe harbours. Finally, the court held that, in accordance with EU and Italian law, CloudFlare cannot require particular formalities as regards the format of notices made to it of illegal activities, other than detailed information of the type of offence detected.

Why it should be listed on the Watchlist

Justanotherpanel is the largest player that we have identified in the global streaming manipulation landscape, with over 1,000 connected domains.

Streaming manipulation generally is of concern to the industry because, as explained above, it diverts streaming royalty payments away from artists whose music was 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 by influencing algorithmic playback results.

The provision of artificially generated streams, regardless of the method of creation, not only breaches the terms of service of major music streaming services, but also deprives rights holders of their rightful royalties and misleads consumers. This activity can lead to both criminal (fraud) and civil liability for the perpetrator in several territories, proven by several courts in Germany having ordered streaming manipulation services to cease offering music streaming manipulation services on the basis that their activities violate unfair competition law, and that actions by law enforcement in Brazil have resulted in the closure of streaming manipulation services.

This illegal activity is a growing problem for the music industry as it diverts revenue away of the rights holder and undermines the legitimacy of the streaming economy. IFPI is focused on tackling this issue before it grows any larger and the most efficient way to do so would be to stop the activity that is generated from the JAP service and its associated network of sites.

According to SimilarWeb[49] JAP received 713.8K visits from October to December 2021, with its top traffic coming from Spain, India, the USA, Georgia and the UK.

[49] www.similarweb.com