EUROPEAN
COMMISSION

Brussels, 1.12.2022
SWD(2022) 399 final

COMMISSION STAFF WORKING DOCUMENT

Counterfeit and Piracy Watch List

TABLE OF CONTENTS

1. INTRODUCTION

Infringements of intellectual property rights (IPR), in particular commercial-scale counterfeiting and piracy, pose a serious problem for the European Union (EU). IPR infringements not only cause high financial losses for European rightholders and undermine sustainable IP-based business models. They also pose a major threat to public health and the society at large, for instance in the form of counterfeit medicines, medical supply and equipment.

In terms of economic harm, the joint study by EUIPO and OECD of June 2021[1] reports that **USD 464 billion** worth of counterfeit and pirated goods were traded worldwide. In the EU, **5.8% of all imports** from third countries are now estimated to be counterfeit and pirated goods, worth up to **EUR 119 billion** (USD 134 billion), a volume that is stable. Top provenance economies in terms of their propensity to export counterfeit products are: Hong Kong (China), China, Singapore and United Arab Emirates.

The study on the *Misuse of E-Commerce for Trade in Counterfeits* by EUIPO and OECD of 2021[2] shows the increase in the number of companies engaged in business to consumer e-commerce. Between 2018 and 2020, online retail sales rose by **41% in major economies,** compared to less than a 1% rise in total retail sales. With respect to provenance, the sources of counterfeits were similar for those linked to e-commerce and those that were not; however, China's share of the total was higher in the case of counterfeits linked to e-commerce (75.9% vs. 45.9% of total number of detentions). The EU detentions of counterfeits linked to e-commerce included a broad range of products, led by **footwear (33.7% of total detentions), clothing (17.3%), perfumes and cosmetics (9.6%), leather articles (8.7%), electrical machinery and equipment (6.5%), toys (5.5%) and watches (5.2%).**

The joint report by DG TAXUD and EUIPO on the *EU Enforcement of Intellectual Property Rights*[3] of November 2021 showed that fake products with a value of almost EUR 2 billion were seized in the EU's internal market and at external borders in 2020. The customs authorities seized at EU external borders 27 million individual items that infringed on IPR. Clothing accessories were the leading category, both in terms of the number of items detained and estimated value, followed by packaging materials; recorded CDs/DVDs; labels, tags and stickers; and clothing. As in previous years, China is the main source third country for the majority of fake and counterfeit goods entering the EU in 2020, followed by Hong Kong (China) (the main source of mobile phones and accessories, as well as labels, tags, stickers) and Türkiye (the main source of clothing, medicines and clothing accessories). Postal, express and air transport remain the most significant means of transport in terms of the number of consignments registered.

[1] *Global Trade in Fakes: A WORRYING THREAT*, 2021_EUIPO_OECD_Trate_Fakes_Study_FullR_en.pdf (europa.eu)

[2] https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/misuse-e-commerce-trade-in-counterfeits/EUIPO_OECD_misuse-e-commerce-trade-in-counterfeits_study_en.pdf

[3] EU enforcement of IP rights: a joint report with the European Union Intellectual Property Office (europa.eu)

The EUIPO report on *Risk and Damages Posed by IPR Infringement in Europe*[4] of June 2021 highlights that 70% of Europeans shopped online in 2020, according to Eurostat. Consumers find it difficult to distinguish between genuine and fake goods, especially online; on average nearly 9% of Europeans claimed that they were misled into buying counterfeits. Counterfeit products impact every sector, from cosmetics and toys, wine and beverages, electronics and clothing to pesticides and pharmaceutical products. The worldwide trade in counterfeit pharmaceutical products had been estimated at **EUR 4 billion**. According to the same report, digital piracy represents a highly lucrative market for infringers. In the area of internet protocol television (IPTV), **EUR 1 billion of unlawful revenue** is generated every year by the supply and consumption of copyright-infringing digital content in the EU. These services were used by 3.6% of the EU population. Around **35%** of digital related public conversations on social media could possibly relate to piracy, with film and music piracy being the areas most discussed, especially on Reddit and Twitter. **More than 670 000 jobs are lost every year** in the EU in 11 key sectors particularly vulnerable to counterfeiting. 3% of companies who own IP rights, such as trademarks or patents, reported a general loss in turnover, while 27% reported damage to their reputation and 15% reported a loss of competitive edge due to IP infringement.

Other studies show the economic harm of piracy on the creative industries. According to some resources looking into the trends in online piracy[5], there has been an increase of 29.3% of visits to piracy websites in Q1 2022 compared to Q1 2021, with the biggest increase in the publishing sector (dominantly for Manga content), followed by film and TV content. According to a 2021 report by recording industry[6], 30% of listeners used unlicensed or illegal ways to listen to the music[7].

In terms of risks to health, consumers and the society, the EUROPOL-EUIPO joint report on *Intellectual Property Crime Threat Assessment* of March 2022[8] provides further insights[9] into the current state and trends of dangerous counterfeits and highlights among other things the increasing role of the digital domain in the distribution of counterfeit products (both tangible and non-tangible) to consumers via online platforms, social media and instant messaging services.

The joint OECD-EUIPO *Report on Dangerous Fakes*[10], focusing on foodstuffs, pharmaceuticals, cosmetics and goods' categories, reveals that the most commonly traded

[4] Risks and damages posed by IPR infringement in Europe (europa.eu)

[5] MUSO Discover Q1 2022 Digital Piracy Data Insights

[6] IFPI-Engaging-with-Music-report.pdf

[7] http://lacoalicion.es/wp-content/uploads/executive-obs.piracy_en_2019.pdf

[8] Intellectual Property Crime Threat Assessment 2022 | Europol (europa.eu)

[9] In addition to the EUIPO's *Qualitative Study on the risks posed by counterfeiters to consumers* that was referenced in the 2020 Watch List, available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers_Study/2019_Risks_Posed_by_Counterfeits_to_Consumers_Study.pdf

[10] dangerous-fakes_study_en.pdf (europa.eu)

product categories of dangerous fakes were perfumery and cosmetics, clothing, toys, automotive spare parts and pharmaceuticals. Most of these goods originated in China (55% of global customs seizures) and Hong Kong (China) (19%). Among dangerous fakes ordered online, cosmetics items were the most common, followed by clothing, toys and automotive spare parts. Most of these goods (75%) were shipped from China. The COVID-19 pandemic has affected trade in dangerous fake goods, and, in most cases, the crisis has aggravated existing trends.

With regard to the link between counterfeiting and organised crime, the new *Internet Organised Crime Threat Assessment*[11] prepared by Europol in 2021 reports further evolutions since the last report of 2019[12] and indicates that in addition to being successfully opportunistic, criminals have continued to mature in their methods and organisation. Cybercriminals continue to move towards a more calculated target selection and there is a rise in ransomware affiliate programs seeking cooperation with hackers and other malware developers. Ransomware operations are becoming increasingly focused on high-value attacks on large organisations and their supply chains.

The Joint Study by Europol and the EUIPO on IP crime and its link to other serious crime[13], cited in the 2020 Watch List, remains relevant in this context by highlighting the negative impact of piracy on consumers and the security of their devices and the personal data and other information stored therein. Along with pirated content, infringing websites commonly distribute various kinds of malware and potentially unwanted programs, luring users into downloading and launching these files. These programs use deceptive techniques and social engineering to trick end-users into disclosing their sensitive information or payment card details[14]. Social engineering has evolved, now equipped with artificial intelligence (AI) tools to further exploit human psychology and gain access to systems and data. However, AI also offers tools for real-time analysis of data and actions and prevention of social engineering attacks. A paper[15] on the impact of piracy on computer security found that the more users visited piracy sites, the more often their machines got infected with malware. Specifically, whenever they doubled the time they spent on piracy sites, they increased the number of malware processes running on their machines by 20%.

In accordance with the Commission's Communication *"A balanced IP enforcement system responding to today's societal challenges"*[16], the *"Trade for all"*

---

[11] internet_organised_crime_threat_assessment_iocta_2021.pdf (europa.eu)

[12] https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019

[13] https://www.europol.europa.eu/publications-documents/ip-crime-and-its-link-to-other-serious-crimes-focus-poly-criminality

[14] *Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites:* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Malware_Study/2018_Malware_Study_en.pdf

[15] https://techpolicyinstitute.org/2018/03/13/piracy-and-malware-theres-no-free-lunch/

[16] COM(2017) 707 final

Communication[17], *the IP Action Plan*[18] and the *Strategy for the Enforcement of Intellectual Property Rights in Third Countries*[19], the Commission services have prepared this third edition of the Counterfeit and Piracy Watch List ('the Watch List'). The first edition was published in 2018 and the second in 2020. The Watch List reflects the results of stakeholder consultations. It contains examples of reported marketplaces or service providers whose operators or owners are allegedly resident outside the EU and which reportedly engage in, facilitate or benefit from counterfeiting and piracy.

As a separate category, the document also mentions service providers which are not reported as having engaged in unauthorised activities, but are mentioned in this Watch List for the reason that they are reported to allegedly lag behind in efforts to combat piracy or counterfeiting (e.g. by not applying industry standards and best practices, recommendations or voluntary measures to prevent or stop the availability of unauthorised IP-protected content in the services or marketplaces they operate).

The aim of this Watch List is to encourage the operators and owners, as well as the responsible local enforcement authorities and governments to take the necessary actions and measures to reduce the availability of IPR infringing goods or services on these markets. In this context, the Commission services will continue using the Watch List in their cooperation with EU's trading partners in the framework of IP Dialogues and Working Groups and in the framework of the EU technical cooperation activities, including IP Key China[20], Southeast Asia[21] and Latin America programmes[22].

The Watch List also intends to raise consumer awareness concerning the environmental, product safety and other risks of purchasing from potentially problematic marketplaces.

The Watch List is a Commission Staff Working Document. Commission Staff Working Documents are factual and informative documents that **do not have any legal effect** and **that do not commit the European Commission.**

The Watch List is a selection of marketplaces and service providers reported by stakeholders. The name of each marketplace and service provider mentioned is accompanied by a short summary of the allegations of the reporting stakeholders and, where provided, a summary of the response of the mentioned marketplace or service provider to those allegations. The European Commission does not take any position on the content of such allegations and the responses to these allegations.

The Watch List is not an exhaustive list of the reported marketplaces and service

[17] COM(2015) 497 final

[18] COM(2020) 760 final. The Commission presented a comprehensive package of actions in the Communication on *Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recovery and resilience* on 25 November 2020: https://ec.europa.eu/docsroom/documents/43845

[19] COM(2014) 389 final

[20] https://ipkey.eu/en/china

[21] https://ipkey.eu/en/south-east-asia

[22] https://ipkey.eu/en/latin-america

providers and does not contain findings of legal violations. The Watch List is limited to reporting on the allegations made by stakeholders and the replies provided by the marketplaces and service providers concerned. The Commission services made every effort to ensure that the information contained in the Watch List reflects accurately and comprehensively the views gathered from all the stakeholders that have participated in the consultation process. The Commission services made every effort to ensure that the information contained in the Watch List is accurate to the best of their knowledge and duly verified, notably through close cooperation between all the relevant Commission services, and the involvement of the European Union Agency for Law Enforcement Cooperation (Europol).

The Commission services made every effort to gather the views of the operators of the relevant marketplaces and service providers included in this Watch List. The Commission services provided them with the opportunity to be heard. In particular, the Commission services invited all relevant stakeholders to submit written contributions to the public consultation launched in December 2021 and following the publication of the submissions, also invited interested stakeholders to make comments on the submissions received.

Moreover, the Commission services proactively reached out to a number of online service providers and marketplace operators to verify information received through the public consultation, where needed. The Commission services took duly into account the comments received from the marketplaces and service providers on the allegations made against them by other stakeholders when drawing up this Watch List. The comments of the service providers and marketplace operators mentioned in this Watch List are summarised together with the allegations of reporting stakeholders.

The Commission services remain available to receive further comments on the information reported in this Watch List as well as requests to rectify this information (e-mail to TRADE-COUNTERFEIT-AND-PIRACY-WATCH-LIST@ec.europa.eu) and will take them into account when regularly updating it in the future.

The Watch List does not provide the Commission services' analysis of the state of protection and enforcement of IPR in the countries connected with the mentioned marketplaces and service providers. A general analysis of the protection and enforcement of IPR in third countries can be found in the Commission services' separate biennial *Report on the protection and enforcement of intellectual property rights in third countries (Third country report*), the latest of which was published on 27 April 2021[23].

[23] *Report on the protection and enforcement of intellectual property rights in third countries* - https://trade.ec.europa.eu/doclib/docs/2021/april/tradoc_159553.pdf

2. METHODOLOGY

2.1. Sources

The Commission services conducted a public consultation between 15 December 2021 and 14 February 2022[24]. Its results form the basis of this Watch List. 77 respondents contributed to the public consultation[25]. The majority of them were brand owners, copyright holders, associations and federations representing rightholders and associations fighting against IP infringements. Other respondents were individuals, law firms and chambers of commerce. A number of online service providers, such as e-commerce and social media platforms, providers of internet infrastructure services or associations of providers of technology products and services also contributed to the public consultation. Information regarding the respondents and their contributions were published[26] on 8 March 2022. Interested stakeholders were invited to submit their observations on the contributions until 5 April 2022 and the observations received were also published[27].

The Commission services made every effort to verify the factual statements contained in the contributions to the public consultation against impartial and reliable sources as indicated in this Section, and including court decisions in the EU Member States and in third countries, where publicly available.

In addition to the support provided by Europol and EUIPO, a number of other sources also played a role in the selection process and in defining and describing the marketplaces and service providers mentioned in this Watch List.

Information from the Commission services

- Information received from EU Delegations and Offices;
- Information on IP policy received from Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs and from Directorate-General for Communication Networks, Content and Technology;
- Information received from the Directorate-General for Taxation and Customs Union on customs enforcement of intellectual property rights by EU Member States[28];
- Information gathered via IP Key Latin-America and IP Key South-East Asia.

EUIPO reports and studies

- Studies on the economic impact of counterfeiting and piracy and trade in fakes[29];

[24] For further details on the public consultation, see Section 3.

[25] Public consultation on the Counterfeit and Piracy Watch List (europa.eu)

[26] consultations - Library (europa.eu)

[27] consultations - Library (europa.eu)

[28] *Report on the EU customs enforcement of intellectual property rights* - https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_EU_enforcement_intellectual_property_rights/2021_EU_enforcement_intellectual_property_rights%20_FullR_en.pdf

[29] *Global Trade in Fakes: A WORRYING THREAT*, 2021_EUIPO_OECD_Trate_Fakes_Study_FullR_en.pdf (europa.eu); *Misuse of E-Commerce for Trade in Counterfeits* by EUIPO and OECD, https://euipo.europa.eu/tunnel-

- Studies on the harm of piracy and counterfeiting to consumers[30];
- Sectoral Studies[31];
- Study on Infringing Online Business Models[32];
- Study on Digital Advertising on Suspected Infringing Websites[33];
- Study on Illegal IPTV in the European Union – Research on Online Business Models infringing intellectual property rights[34];
- Joint Study by EUIPO and Europol on IP crime and its link to other serious crime[35].

Other relevant sources

- Europol crime threat assessments[36];
- SimilarWeb[37] popularity ranks;
- Google Transparency Report[38];

---

web/secure/webdav/guest/document_library/observatory/documents/reports/misuse-e-commerce-trade-in-counterfeits/EUIPO_OECD_misuse-e-commerce-trade-in-counterfeits_study_en.pdf; the joint report by DG TAXUD and EUIPO *EU enforcement of IP rights: a joint report with the European Union Intellectual Property Office (europa.eu)* ;the EUIPO report *Risks and damages posed by IPR infringement in Europe (europa.eu)*

[30]EUROPOL-EUIPO joint report on *Intellectual Property Crime Threat Assessment*, internet_organised_crime_threat_assessment_iocta_2021.pdf (europa.eu), ; OECD-EUIPO *Report on Dangerous Fakes*, *dangerous-fakes_study_en.pdf (europa.eu)*

[31] EUIPO's study on Q*uantification of IPR infringements*,https://euipo.europa.eu/ohimportal/fr/web/observatory/quantification-of-ipr-infringement

[32] Research on *Online business models infringing intellectual property rights*, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf

[33] Study on *Digital advertising on suspected infringing websites*,https://euipo.europa.eu/ohimportal/documents/11370/80606/Digital+Advertising+on+Suspected+Infringing+Websites

[34] *Illegal IP TV in the European Union - Research on online business models infringing intellectual property rights,* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf

[35] *Joint study by EUIPO and EUROPOL IP CRIME AND ITS LINK TO OTHER SERIOUS CRIMES Focus on Poly-Criminality*

[36] Europol's report on *Internet organised crime threat assessment* s of 2019 and 2021 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 ; internet_organised_crime_threat_assessment_iocta_2021.pdf (europa.eu)

[37] The EUIPO's *Study on Digital Advertising on Suspected Infringing Websites* describes that "*SimilarWeb uses big data technology to estimate websites' unique visitors from desktops and the origin of those visits. SimilarWeb provides information on: (1) global rank, rank of site in top country, and category rank (i.e. Rank 15 in the category of File Sharing), as well as the up or down trend in popularity; (2) total visits each month for the past 6 months; (3) traffic sources (35% direct, 33% referrals, 14% search, 7% social); (4) top 5 referring sites and top 5 destination sites; (5) leading organic keywords that users searched that led them to the site; (6) percentage of social networks sending traffic to the site; (7) top ad networks and leading publishers referring advertising traffic to the website; (8) audience interests including a short list of websites frequently visited by the website's users; (9) similar sites and (10) related mobile apps*".

- Reports and assessments made by other relevant bodies and organisations (e.g. the OECD).

2.2. Selection

The selection of the marketplaces and service providers in the Watch List aims to provide significant examples of different types of online service providers and physical markets that play, directly or indirectly, a major role in the counterfeiting or piracy of EU IPR-protected goods and content outside the EU. The marketplaces and service providers in the Watch List were selected between April and September 2022. Consequently, the information included in the report reflects the situation during this period.

All selected marketplaces and service providers are located outside the EU to the knowledge of the Commission services. Online marketplaces and service providers are considered to be located outside the EU for the purposes of the Watch List if their operator or owner is known or assumed to be resident outside the EU, irrespective of the residence of the domain name registry, the registrar, the residence of the hosting provider or the targeted country. As regards physical marketplaces, the market is considered located outside the EU if it is physically hosted in the territory of a third country irrespective of the citizenship or residence of its landlord.

Most stakeholders that contributed to the public consultation launched by the Commission indicated the marketplaces and service providers that, in their view, should be included in the Watch List (see Section 3 for further details). Most of the selected service providers were reported in various contributions, often by stakeholders representing a wide array of sectors.

Other stakeholders such as e-commerce, social media platforms, providers of internet infrastructure services or associations of providers of technology products and services also provided their input in the public consultation, including on measures they take to reduce the availability of counterfeit offers and piracy on their platforms.

Some contributions included detailed explanations of the acts performed by the allegedly infringing service providers or service providers' failings as regards the measures taken to fight illegal content or goods on their services. This is sometimes confirmed by decisions of the national courts of the EU Member States and of third countries declaring the liability of, or blocking access to, the service providers.

Some contributions included a qualitative assessment of the harm caused to the EU industries by certain marketplaces and service providers. Their global or regional popularity and their high volume of sales of counterfeit or pirated content were also examined. In order to identify websites that are popular globally or regionally, SimilarWeb web popularity ranking and Google's Transparency Reports[39] for copyright-

[38] https://transparencyreport.google.com/ Google makes available online a report that indicates the volume of infringement takedown requests sent by parties to Google for search takedowns in relation to websites that may infringe copyright. The listed copyright related websites were cross-checked with the Google Transparency Report for specific organisations to identify websites with the highest number of infringing link notices sent to Google by key IP rightholders and other IP content protection associations.

[39] https://transparencyreport.google.com/copyright/overview?hl=en

related websites were used. Some of the selected marketplaces or service providers are mostly visited from the EU whereas others are visited only from third countries but harm EU rightholders and trade with these countries. Searches for popular European content titles or brands were also carried out in order to verify the availability of suspected copyright-infringing content or suspected counterfeit goods.

Measures taken by online service providers with regard to the principles recommended in the Commission's *Recommendation on measures to effectively tackle illegal content online*[40] (e.g. the need for a clear notification procedure, transparent policy for the removal or disabling access to the content, regular activity reports, the use of automated means for the detection of illegal content, cooperation with rightholders and enforcement authorities) were reported by stakeholders and also taken into account in the preparation of the Watch List.

The recently adopted Digital Services Act[41] ("DSA") provides for new legal obligations on certain online services[42], including e-commerce platforms (online marketplaces), concerning measures or action to be taken by them with regard to illegal content. The DSA includes greater obligations for very large platforms and very large online search engines. These new rules are not yet applicable[43], but already give some additional indications of what type of diligence could be expected from certain online service providers.

The Commission is also developing an EU Toolbox against counterfeiting, which will complement and build on ongoing and upcoming legislative initiatives such as the DSA, by further implementing the new legal framework, highlighting good practices in the fight against counterfeiting, supporting SMEs in enforcement of their IP rights and promoting the use of new technologies to address IPR infringements.

This edition of the Watch List does not contain updates on online service providers or marketplaces reported for Ukraine, without prejudice to possible concerns with these services or marketplaces.

3. RESULTS OF THE PUBLIC CONSULTATION

Like in previous years, creative industries covering a wide array of sectors, such as music, audiovisual, publishing, TV broadcasting or software, submitted most of the

[40] *Commission Recommendation on measures to effectively tackle illegal content online* https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[41] EUR-Lex - 32022R2065 - EN - EUR-Lex (europa.eu)

[42] For the sake of this Watch List the terms 'online service providers' and 'e-commerce platforms' are maintained while it is to be noted that in recently adopted legislation, including the DSA, these services are referred to as online intermediary services and online marketplaces.

[43] The DSA will apply to very large online platforms and very large online search engines four months after their designation and to other providers of intermediary services falling within the scope of the DSA on 16 February 2024.

public consultation contributions on piracy. The contributions from broadcasters or organisers of broadcast sport events remained numerous as well, showing a continuous and an increasing concern about the proliferation of operators engaged in the provision of unlicensed IPTV services.

As in previous years, linking websites and cyberlockers were widely reported together with unlicensed IPTV operators, peer-to-peer networks and BitTorrent indexing websites and stream-ripping services. Some new services and trends were reported, such as services supporting piracy by offering off-the-shelf services that make it easy for would-be pirates to create, operate, and monetise a pirate operation. Reference was also made to potential copyright infringements in the context of the metaverse, which may require further monitoring in the future.

Brand owners (electronics, fashion, footwear, luxury, sporting goods, toys, etc.), brand associations and federations, chambers of commerce, associations fighting against counterfeiting reported mostly physical marketplaces and e-commerce platforms. More than 40 e-commerce platforms were reported for the online distribution of allegedly counterfeit goods.

Respondents to the public consultation continued to show concerns about the significant role of certain actors in addressing proliferation of pirated content, such as providers of ad networks and social media, as well as Content Delivery Networks[44] (CDNs). The debate on the expected diligence of these different service providers with regard to fighting piracy and counterfeiting is ongoing and some new rules set by the DSA may bring further clarity alongside the evolving case law.

As an example, like in 2020, the US-based *Cloudflare*, has again been reported this year by some stakeholders calling on the service to improve further its cooperation with rightholders, including its responsiveness to infringement notices, repeat infringer policy, and its practices when opening accounts for websites to prevent illegal sites from using its services ("know your customer policy"). Cloudflare referred to the erroneous characterisation of their reverse proxy cybersecurity services and CDN services as "hosting" services and stated that they did not host material, which makes it impossible for them to remove particular pieces of content from the Internet when their reverse proxy or CDN services are used. They referred to the 2021 court decision from the U.S. District Court for the Northern District of California[45] regarding CDN services, which concluded that Cloudflare's security and caching services do not materially contribute to copyright infringement. Cloudflare also reported on the steps they take to avoid

[44] A Content Delivery Network is a geographically distributed network of proxy servers and their data centres that replicates a website's content on each of the servers to allow the downloading of the content from the place that is closest to the user. CDNs increase content delivery speed and capacity and provide security against threats such as hacking or viruses. CDN reverse proxy services protect websites' IP addresses in order to prevent cyberattack. This affects the information provided by the WhoIs Database (an online protocol that is widely used for querying databases that store registered data on the users of a domain name, the IP address, the name of the registrar, starting date and expiration date of the domain name, etc.). For websites using CDNs, WhoIs lists the IP address of the server within the CDN (front host) through which the content is routed and not the server actually hosting the content (back host).

[45] Mon Cheri Bridals, LLC v. Cloudflare, Inc., Case No. 19-cv-01356-VC (N.D. Cal. Oct. 6, 2021)

infringements, through their abuse reporting system[46], which passes on complaints of copyright violations to the website owner and Trusted Reporter programme[47], to ensure that rightholders have the necessary information to pursue complaints of alleged infringements with the hosting providers and website operators, which are able to act on those complaints. Cloudflare also reported to respond to complaints with information about the hosting provider so that complainants can follow up directly as necessary. Rightholders reported a new preliminary injunction issued by an Italian court[48].

Stakeholders from different sectors also continued to report concerns with regard to *Telegram* for features that allow users to share unauthorised content with a significant number of users through a group or via channels for broadcasting to unlimited audiences[49]. Stakeholders notably report insufficient responsive action from Telegram when they notify infringements. Telegram from their side indicated that they collaborated with industry leaders, governments, and policymakers worldwide on a regular basis, introducing automated content monitoring systems and adopting other industry-wide best practices. Apart from user reporting mechanisms in place (such as in channels or bots), there is also an option to contact *@NoToScam* or submit a complaint via e-mail by the copyright owner or an agent authorised to act on the owner's behalf. Reports (including for copyright infringements) are processed 24/7 and this comprises reports from users made via Telegram app, as well as email reports from non-registered users and trusted flaggers.

Respondents to the public consultation continued to express concerns about the role of certain social media platforms in the distribution of counterfeit goods online. The Transnational Alliance to Combat Illicit Trade (TRACIT) stated that since their report of 2020[50], the problem has shown no signs of slowing and observed that the numbers of fraudulent advertisements on social platforms were going up, not down.

A number of online services were reported by stakeholders in the context of ad networks supporting illegal activities. Some specific domain name registries have also been

[46] Abuse approach - Cloudflare | Cloudflare

[47] Cloudflare reports that their abuse reporting system and Trusted Reporter programme demonstrate the cooperation with rightholders. For instance, while their abuse reporting process is available to everyone, Cloudflare has built an API that enables frequent reporters to automate the submission of abuse complaints. Cloudflare has also built a Trusted Reporter programme, designed for large rightholder organisations who have demonstrated a need for additional information and a capacity to protect sensitive information. Along with law enforcement agencies, their Trusted Reporter programme consists of more than 40 major intellectual property rightholders and rights organisations in Europe.

[48] 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. Order issued by the Court of Rome XVII (formerly IX) Civil Section, on 24 June 2019 - R.G.26942/2019. On 11 July 2022, the Court of Milan issued a preliminary injunction (R.G. 50126/2021) against Cloudflare ordering them to block the DNS resolution of some pirate torrent websites.

[49] See description of Telegram's services at Telegram FAQ

[50] TRACIT study on *Fraudulent advertising online – Emerging risks and consumer fraud* - https://www.tracit.org/featured-report-fraudulent-advertising-online.html

reported by rightholders, as not taking sufficient measures to avoid registration of pirate websites (.to, .ru, .tv, .bz, .io).

Some e-commerce and social media platforms, as well as other online service providers provided detailed information on the measures they take to reduce the availability of counterfeit offers and piracy on their platforms. A number of e-commerce platforms rely partly on the key performance indicators introduced by the *Memorandum of Understanding on the sale of counterfeit goods via the internet*[51], which is a voluntary agreement facilitated by the European Commission to prevent offers of counterfeit goods from appearing in online marketplaces.

With regard to illicit online pharmacy networks, stakeholders reported that the practices described in the previous Watch List continue, notably the use of domain privacy and proxy services for domain registrations, the use of subdomain to conceal infringing content and the registrations of hundreds of websites funnelling the traffic. Significantly fewer networks and registrars than before were reported in the public consultation for this Watch List, with scarce substantiation of the claimed facts. For this edition, the Commission services therefore refrain from mentioning specific networks.

In some countries, medicines are available via social media platforms or in unregulated open markets, for instance, alongside other day-to-day consumer items. Counterfeit medicines affect the global population but there is a noticeable prevalence of counterfeits including lifesaving medicines, such as antibacterial or antimalarial medicines, in the African region.

For some markets, stakeholders have indicated that sellers make counterfeits available online as well. In part, this may be the result of temporary physical markets' closures during the COVID-19 pandemic or the concomitant drop in the number of tourists purchasing on these markets.

4. POSITIVE DEVELOPMENTS SINCE THE 2020 WATCH LIST

Since the 2020 Watch List, several enforcement actions and measures have been taken by enforcement authorities, rightholders and the owners, operators and landlords of marketplaces and online service providers, partly as a consequence of the Watch List. Some of the marketplaces or service providers mentioned in the 2020 Watch List are therefore no longer mentioned in this Watch List. Others may be not mentioned, despite continued concern expressed by rightholders, for reasons such as their diminished popularity or relevance. The Commission services welcome these actions and measures and encourage enforcement authorities, rightholders and the owners, operators and landlords to continue combating piracy and counterfeiting. The following sections give concrete examples of these developments.

[51] *Memorandum of Understanding on the sale of counterfeit goods on the internet* (the territorial scope of the MoU is limited to the activities of the signatories within the EU/EEA), https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en

Positive developments by e-commerce platforms

Mercado Libre

Mercado Libre has taken significant further steps to improve their measures against counterfeiting and piracy. As reported by Mercado Libre, they have put in place a Brand Protection Portal that offers a streamlined, state of the art reporting tool and comprehensive case management system for IP protection across all 18 Mercado Libre marketplace sites. The program provides a "one-stop" destination for rightholders of all sizes to easily record and enforce a variety of IPR. The Brand Protection Portal includes both reactive measures (facilitating removal of infringing listings based on notices submitted through a reporting tool) and proactive measures (facilitating removal of infringing listings based on artificial intelligence and machine learning technologies). The portal also facilitates enforcement efforts by providing rightholders a free and easy-to-use tool to monitor and report suspected infringing listings on Mercado Libre sites. Additionally, Mercado Libre launched in 2021 a Know Your Customer (KYC) initiative that strengthens their procedures to validate the identities of registered users of Mercado Libre and Mercado Pago[52] accounts including both natural and legal persons. Mercado Libre has also stepped up their cooperation with rightholders through the launch in November 2021 of the Anti-Counterfeiting Alliance, which is a partnership between the company and different rightholders to fight together against the online trading of illicit goods in Mercado Libre's ecosystem. Finally, Mercado Libre is regularly making available a transparency report on their actions, with the first report published early 2021.

Snapdeal

Snapdeal has demonstrated important progress in their policies and implementation of mechanisms against counterfeits and piracy. Over the last two years, Snapdeal's brand protection program has incorporated various features in order to prevent, protect against and deter counterfeiting and piracy, including keyword blocking, notice and take down procedures, seller identity verification, proactive identification of counterfeit goods, brand alliances, and employee training. They have reported in detail on the different measures and cooperation with brand owners, industry associations and law enforcement authorities. Snapdeal has also indicated its commitment to engaging with its peers and other stakeholders to increase its anti-counterfeiting measures.

Bukalapak

Bukalapak has provided detailed information about the different measures taken to address counterfeiting and piracy, which addressed the concerns expressed by rightholders, supported by data. They have in particular reported on their proactive measures that rely on the use of industry leading filtration technology and collaboration with brand owners, associations and governments, as well as their 'know your customer' requirements applied to sellers, who register and sell their products on their platform. They have reported on the availability of several channels to submit counterfeit and

[52] The fintech platform of Mercado Libre

piracy complaint reports (including a bilingual Form 175)[53] and on a shortened average resolution time for notices and complaint processing.

Positive developments concerning online services

Bookfi.net – an important website of the Library Genesis Project seems to be offline now.

Electrotv-sat.com – included in the previous Watch List under illegal IPTV services, seems to be offline due to copyright infringements.

Wi.to – a cyberlocker reported in 2020, does not seem to be available any more.

Youtubeconverter.io – included in the previous edition of the Watch List as linked to the stream ripping service Y2mate, does not seem to be available any more.

Popcorn Time – an application for mobile phones, tablets, and other streaming devices that aggregates bit torrent files for streaming pirated movies and has been reported in previous editions of the Watch List seems to have lost its popularity[54] even if it still exists and has been reported by stakeholders.

Actions taken by public authorities

South Korean authorities have reported on their actions taken with regard to physical marketplaces and cooperation with online services. According to their report, the Korean Intellectual Property Office (KIPO) has held meetings with online markets and physical markets to check the allegations reported by rightholders and to consider a plan for improvements. With regard to physical markets, they reported a sharp increase in the number of seizures.

Several regional or national developments were reported in the context of the EU funded technical cooperation programmes - IP KEY Latin America and South East Asia. For example, in Malaysia, the Ministry of Domestic Trade and Consumer Affairs officially launched in January 2022 the Cyber Copyright Enforcement (CyCORE) programme, aimed at combatting digital film copyright infringement in Malaysia.

In Vietnam, on 9 December 2021, the Vietnam Digital Content Copyright Center ("VDCC") under the Department of Radio, Television and Electronic Information (under the Ministry of Information and Communications), was officially established. On their website a complaint section[55] is available for the public to make complaints about any piracy in the digital environment.

According to the news[56], the Indonesian Ministry of Tourism and Creative Economy (Kemenparekraf) together with the Indonesian Publishers Association (IKAPI) have

[53] https://bukabantuan.bukalapak.com/form/175

[54] Popcorn Time Alternative Is Hard to Find as App Shuts Down - Bloomberg

[55] https://banquyen.gov.vn/khieu-nai-phan-anh/

[56] As published in the online news https://nasional.kontan.co.id/news/marak-pelanggaran-hki-ini-yang-dilakukan-pemerintah-untuk-berantas-barang-bajakan

made efforts to prevent the sale of pirated books on digital platforms, by inviting marketplace organisers to create a screening system. Kemenparekraf has facilitated the signing of a memorandum of understanding between IKAPI and Tokopedia in an effort to prevent the sale of pirated books on Tokopedia.

5. ONLINE SERVICE PROVIDERS OFFERING OR FACILITATING ACCESS TO COPYRIGHT-PROTECTED CONTENT

Online services remain the main source of copyright infringements. Various types of online service providers provide access to copyright-protected content, such as music, films, books and video games, without authorisation of the rightholders. These service providers rely on other online service providers, such as reverse proxy services, caching services, hosting providers, ad networks and payment services to carry out their activities. Certain online service providers also contribute directly or indirectly to copyright infringements by facilitating access to unauthorised content made available by third parties or providing devices and products or services to circumvent technological protection measures used by rightholders to prevent or restrict unauthorised acts.

This section lists service providers that offer content protected by copyright and service providers that directly or indirectly facilitate access to this content. Some of the mentioned service providers were reported because they do not apply practices that prevent or substantially reduce the risk of their services being used for the purposes of infringing copyright. The service providers are grouped in sub-sections according to their business model and type of service they provide, following a structure similar to the one used in the previous editions of the Watch List. It also contains a new subsection for a new type of service reported by stakeholders as supporting piracy.

5.1. Cyberlockers

A cyberlocker is a type of cloud storage and cloud sharing service that enables users to upload, store and share content in centralised online servers. The owner of the website manages the content. Cyberlockers generate a unique URL link (or sometimes several URL links) to access the uploaded file, enabling clients to download or stream the uploaded content. Content stored in cyberlockers may be protected by copyright or not. However, if a user uploads copyright-protected content and shares the URL link, others can download that content without the authorisation of the rightholder.

Stakeholders report different ways used by cyberlockers listed in this section to facilitate wider distribution of illegal content. For example, they incentivise and reward their users to upload popular files to their servers. The rewards offered depend on the size of the downloaded file, the location of the downloader and the number of times users download or stream the uploaded content. Moreover, the URL links to the infringing content are usually promoted across the internet by different means, such as social media platforms, blogs, emails, mobile applications or links in other websites, including linking and referring sites (see Section 5.3 below). This, according to the film, TV, music, software and book publishing industries, makes the listed cyberlockers an important part of the ecosystem that facilitates widespread access to high volume of infringing content uploaded anonymously onto their servers. Finally, stakeholders report that the listed cyberlockers usually mask the identity of their operators via domain privacy services or

corporate structures involving various states. Moreover, they often generate several unique links to the same file and use proxy servers to hide the locations of the hosted content. This makes it hard for enforcement authorities to link these sites to any natural person.

Some new trends in cyberlocker piracy have been reported this year. The music industry reports that in the last few years, cyberlockers have again increased in popularity - in Q4 2021, the International Federation of the Phonographic Industry (IFPI) tracked 1.35 billion music-focused visits to cyberlockers, an increase of 5.2 percent compared to the same period in 2020. IFPI also 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, they report that cyberlockers remain a major distribution channel for leaked pre-release content.

Stakeholders from various creative industries have reported that the cyberlockers listed below received notices to take down content or cease and desist letters, but they did not react or did not remove the content, even if some of them publish their IP policies.

It is to be noted that the Court of Justice of the European Union (CJEU) decision in the joint cases Uploaded and YouTube (C-628/18, C-683/18) clarifies under which conditions a cyberlocker may be considered to be communicating to the public and therefore be directly liable for copyright infringements.

Mega.nz/.io

Mega was reported for inclusion in the Watch List by stakeholders in the music industry. They report that *Mega.nz* was the most popular site used by respondents for downloading, when presented with a selection of sites which included cyberlockers, stream rippers and BitTorrent sites. *Mega.nz* automatically redirects users to *MEGA.IO*, which is used as a front-end by users, but all infringing content is hosted by the Mega.nz domain. A key feature of *Mega* is that it allows account holders to transfer content directly between accounts. It also 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.

The stakeholders report *Mega* for the lack of preventive measures to avoid uploads of infringing content. According to their information, in January 2022, ISPs in Russia were ordered to permanently block the site following music rightholders' actions.

According to SimilarWeb, *Mega.nz* had a global ranking of 206 and 172.7 million visits in July 2022.

Uptobox - uptobox.com / Uptostream.com

Uptobox has mainly been reported for inclusion in this Watch List by stakeholders in the audiovisual sector.

Uptobox is reportedly a direct download cyberlocker. However, it also allows streaming and embedding via its related site, *uptostream.com*. Uploaded content includes films and videogames, including pre-releases. Its hosting location is masked behind a reverse proxy service, making it difficult to identify its precise host.

The site offers a premium account with unlimited storage, unlimited downloads, extra download speed and no advertisements. Pirate sites embed or link to the content uploaded in *Uptobox* to generate revenues through advertisements or through networks that pay per visited link. Stakeholders report a long response time to notifications of infringements.

According to SimilarWeb, *Uptobox* had a global ranking of 2 100 and 31.9 million visits in July 2022.

Rapidgator - rapidgator.net

Stakeholders across different sectors, including publishing, music and audiovisual, continue reporting *Rapidgator* for inclusion in this Watch List.

Rapidgator provides free and paid for file hosting and sharing services. Its features include "extra fast downloads [and] unlimited file storage". A search engine inside of *Rapidgator* allows users to find copyright protected content. The site's IP address puts it in Russia with its own ISP. As reported in 2020, Russian courts issued a blocking injunction against *Rapidgator* in 2019[57]. However, the site is still accessible from other countries. Legal action concerning *Rapidgator* also includes decisions issued in Germany[58].

Rapidgator reportedly generates approximately USD 21 million in annual revenue[59]. Stakeholders report that *Rapidgator* offers rightholders the possibility of opening accounts in order to report the availability of unauthorised content on the site. *Rapidgator* takes down the content but it allegedly makes no effort to remove other uploads of the same infringing content or to prevent infringing content from being re-uploaded immediately after the takedown. Publishers report that this cyberlocker has been sent hundreds of thousands of takedown requests and remains a significant source of infringement.

Rapidgator had a global SimilarWeb ranking of 1 714 and 32.7 million visits in July 2022.

Uploaded - uploaded.net (ul.to, uploaded.to)

Stakeholders across different sectors, mainly publishing and audiovisual sectors continue reporting *Uploaded* for inclusion in this Watch List.

Uploaded is a direct download cyberlocker, hosted in Germany and allegedly operated from Switzerland. It reportedly offers access to a broad range of infringing content such as books, films, TV programmes and music, including pre-release content. *Uploaded* has a reward scheme in place to generate income and to incentivise the sharing of content. The site rewards users for uploading large files like films and TV programmes and for

[57] Moscow City Court Appeal Ruling 33/150 – 23 January 2019.

[58] District Court of Hamburg, 12 July 2018 – 308 O 224/18 and 23 July 2019 – 310 O 193/19.

[59] https://www.zoominfo.com/c/rapidgator/358482797

high numbers of downloads of their uploaded content. The site is blocked in India[60] and Italy[61].

The CJEU ruled in July 2021 that certain factors present in Uploaded's business model can lead to direct liability but left the final decision to the German Federal Court of Justice, which in June 2022 issued an order[62] that confirmed that there were indications that Uploaded may be liable for copyright infringements but left it for lower courts to assess.

The publishing sector reported that *Uploaded* has been sent hundreds of thousands of takedown requests from publishers and remains a significant source of infringement.

Uploaded.net had a global SimilarWeb ranking of 6 559 and 12.9 million visits in July 2022.

Dbree - dbree.org

The music industry has reported *Dbree* again for inclusion in this Watch List.

This cyberlocker allegedly makes available copyright protected content on the internet without authorisation from copyright holders and derives revenue from advertising. It 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 reported to be frequently found on known leak sites and forums content. It also has a search engine allowing users to search for various artists. Stakeholders report that it has been launched recently but it is capitalising on the popularity of another unconnected cyberlocker, dbr.ee, which shut down in 2019. The operator(s) of *Dbree.org* take several steps to try to hide their identities.

The service is reported by stakeholders to be unresponsive to infringement notices. In November 2021, the Italian Regulatory Authority for Communications (AGCOM) ordered ISPs to block access to *Dbree.org*.

Dbree had a global SimilarWeb ranking of 28 693 and 1.7 million visits in July 2022.

5.2. Stream-ripping services

Stream-ripping services are websites, software and apps that enable users to obtain a permanent copy of audio or audiovisual content by downloading it from online streaming

[60] High Court of Delhi, CS(OS) 1860/2014, 23 June 2014, I.A. No. 11577/2014: http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=119642&yr=2014

[61] Precautionary blocking injunction of the Judge for the Preliminary Investigation (Giudice per le Indagini Preliminari – GIP) of Rome, 27 February 2013.

[62] Der Bundesgerichtshof - Presse : Pressemitteilungen aus dem Jahr 2022 - Zur Haftung von "YouTube" und "uploaded" für Urheberrechtsverletzungen

platforms[63]. Stream-ripping services enable users to copy the URL of content taken from a streaming platform and paste it into a search box on the stream-ripping site. When the user clicks on the download button, the stream-ripping site converts the content and creates a media file. According to the relevant rightholders, this operation usually involves the circumvention of the technological protection measures applied by the streaming platforms.

Stream-ripping services often provide a search function on their platform, so that the user does not need to search for a link on other platforms. Stream-ripping plug-ins usually offer a specific download button placed on the streaming platform, making the ripping of the content even easier for the users.

Stakeholders report that advertising is the main revenue source of stream-rippers, with many disseminating malware to obtain the users' personal data or bank payment details. According to stakeholders, stream-rippers are causing significant losses for the music, film and television industries by having a negative impact on income from legal streaming services and sales from the legal download services.

According to the input from the music industry, stream-ripping remains the key music piracy threat. They reported that 35% of 16 to 24 year olds used stream-ripping sites as a way to listen to or obtain music.

A further trend reported by stakeholders is for stream-ripping sites to offer and promote apps on their sites for users to download. Having the app on the site ensures that the app remains available and cannot be subject to removal from the App stores following a complaint by a rightholder.

Y2mate.com, https://www-y2mate.com/ , https://en.y2mate.is

Stakeholders from the music industry continue reporting *Y2mate* for inclusion in this Watch List.

On *Y2mate* users are able to convert and download either an audio-only MP3 file or the entire audiovisual work as an MP4 file through the site. The site also provides users with step-by-step instructions as to how to convert and download files. Following music rightholders' actions, *Y2mate* is currently subject to website blocking orders in Brazil[64], Ecuador[65], Peru[66], Italy[67] and Spain[68]. Stakeholders reported that whilst the operator has

[63] These online streaming platforms may be legal operators that have acquired licences for streaming content. Stream-ripping services allow users of such platforms to download to their devices content that otherwise would only be available through streaming.

[64] On 10 August 2021, the Tribunal of Justice of the State of São Paulo, issued a permanent blocking order against 14 stream-ripping sites including Y2mate.com, Flvto.biz and 2conv.com following an application filed by the Prosecutor's Office Anti-Organized Crime Group (CYBER GAECO), the Prosecutor's Office of the State of São Paulo (DEIC) and APDIF DO BRASIL (the recording industry anti-piracy association).

[65] On 23 July 2021, SENADI (the Ecuadorian Intellectual Property Office) ordered ISPs to block access to four stream ripping websites including Y2mate.com following an application by SOPROFON (the music industry's collective management organisation in Ecuador).

voluntarily geo-blocked *Y2mate.com* from both the US and the UK, the operator has responded by registering the new domain *YT1s.com.*

Y2mate had a global SimilarWeb ranking 296 and 122.9 million visits in July 2022.

Savefrom - Savefrom.net /ssyoutube.com/sfrom.ne

Stakeholders from the music industry have again reported *Savefrom* for inclusion in this Watch List as a stream-ripping service.

Savefrom 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. According to stakeholders, the service has discontinued its offer in the US and the UK following action by rightholders. However, the service continues to operate in other territories outside of the US and UK via the domains *ssyoutube.com* and *sfrom.net*. *Savefrom.net* is subject to a website blocking order in Spain[69].

Savefrom had a global SimilarWeb ranking of 452 and 107.9 million visits in July 2022.

Flvto and 2conv - Flvto.biz and 2conv.com

Stakeholders from the music industry have reported *Flvto* and *2conv* again for inclusion in this Watch List as a stream-ripping service dedicated to the mass-scale piracy of music.

Flvto and *2conv* are allegedly the same service operating from different front-end domains. They are reportedly operated by the same individual in Russia and serve downloads of converted YouTube videos to users as mp3 audio files. Legal action concerning these sites, as reported in 2020, includes judgments or blocking orders in Australia[70], Brazil[71], Ecuador[72], Russia[73], Denmark[74], Italy[75] and Spain[76] and the UK

[66] According to the copy of INCOPI comments under the US Special 301 Report, as published by torrentfreak.com at peru-301.pdf (torrentfreak.com)

[67] Italian Regulatory Authority for Communications, Decision 70/19DDA.

[68] Juzgado de lo Mercantil nº 8 de Barcelona, sentencia nº 27/2020.

[69] On 7 May 2021 the Mercantile Court of Barcelona ordered ISPs to block multiple stream-ripping websites including Savefrom.net following an application by submitted by AGEDI (the music industry's local collecting society). Juzgado de lo Mercantil nº 02 de Barcelona, Procedimiento ordinario (Materia mercantil art. 249.1.4) - 1824/2020 –P.

[70] Federal Court of Australia [2019] FCA 751 – 3 April 2019.

[71] See footnote 65

[72] See footnote 66

[73] The permanent blocking decision in relation to Flvto was issued on 26 April 2019 by the Moscow City Court (case reference No. 3-296/2019). The permanent blocking decision in respect of 2conv.com was issued on 25 June 2019 by the Moscow City Court (case reference No. 3-513/2019).

[74] Court of Aarhus, BS-41534/2018-ARH, 20 December 2018.

Flvto.biz is additionally blocked in Peru[77].

Flvto had a global SimilarWeb ranking of 1 020 and 3.7 million visits in July 2022.

Snappea.com, Sneppea.com/

Stakeholders from the music industry reported *Snappea.com* for inclusion in the Watch List as new fast growing stream ripping service. The service has different functionalities in different locations. It allows to obtain a copy of a YouTube video or 'rip' audio from the video.

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. On 25 August 2022, the Tribunal of Justice of the State of São Paulo, issued a permanent blocking order against all of the stream ripping targets (with the exception of one mobile app which is subject to separate pending proceedings)[78].

According to SimilarWeb, *Snappea* had a global ranking of 23 237 and 2.8 million visits in July 2022.

5.3. Linking or referring websites

Linking or referring websites aggregate, categorise, organise and index links to content that is usually stored on other sites allegedly containing pirated content, including cyberlockers and hosting sites. Linking to third-party sites reduces their maintenance costs. Others, however, host the content files on servers they control.

Linking sites offer search tools and often categorise and organise the content by title, album, genre or, in the case of TV series, season. The users obtain detailed information on the content and can choose to download or stream a film file or a music track or album by clicking on the download or stream button. Then they are redirected to another site, from where the download or streaming starts automatically. Alternatively, the streaming of the content occurs directly on the same website. In this case, instead of providing a text hyperlink, the site may embed or frame the content to stream it in a video player. Some sites also combine lists of links with video players. The linking or referring sites listed below pursue financial gains through income from advertising and referrals.

---

[75] AGCOM Order 114/18/DDA-Flvto.biz of 30 November 2018 and Order 18/19 DDA -2conv.com of 23 January 2019.

[76] Juzgado de lo Mercantil nº 11 de Barcelona, sentencia nº 195/2019.

[77] In April 2021, INDECOPI (the Peruvian IP Protection Authority) issued a preliminary injunction requiring ISPs to block access to a number of stream ripping websites including Flvto.biz following an application by IFPI's local group in Peru, UNIMPRO; RESOLUCIÓN N° 0149-2021/CDA-INDECOPI.

[78] Processo Digital nº: 1012564-72.2022.8.26.0050.

The music and film industries are particularly concerned, since, allegedly, linking sites often make available pre-release content.

Fmovies.to/ https://fmoviesto.site/, https://fmovies.ink/, https://fmoviesto.cc/, https://fmoviesto.hn

Fmovies was reported by audiovisual industry for inclusion in the Watch List. It is reported to be branded also as *Bmovies*, *Bflix*, and other names and to be one of the most popular piracy streaming websites/brands in the world, providing unauthorised access to popular movies and TV series.

The site has been blocked in many countries, including India, Australia, Denmark, Indonesia, Malaysia, and Singapore. The former domain, *Fmovies.se*, was blocked in nine countries.

Fmovies.to had a global SimilarWeb ranking of 720 and 86.5 million visits in July 2022.

Seasonvar - Seasonvar.ru

Stakeholders from the audiovisual industry continue reporting *Seasonvar.ru* for inclusion in this Watch List.

Seasonvar is a Russian-language streaming website that offers free access or a premium subscription that allows users to download or stream HD audiovisual content without any advertising interruptions. On its website it claims[79] to have 21 942 series, 6 689 of these in high-definition and 1 799 with subtitles. The website is allegedly hosted in Russia. Legal action concerning this site includes blocking orders in Russia[80] and Spain[81].

Seasonvar had a global SimilarWeb ranking of 3 186 and 26.3 million visits in July 2022.

Rlsbb - Rlsbb.ru

Stakeholders from the audiovisual industry have again reported *Rlsbb* for inclusion in the Watch List.

This English-language website allegedly facilitates access to a wide range of infringing content by regularly posting articles that contain details about movies and other types of content, together with links to cyberlockers. It is allegedly hosted in the United States. As reported in 2020, legal action concerning this website includes blocking orders in Belgium[82], Denmark[83], Italy[84] and Portugal[85].

[79] In August 2022

[80] Moscow City Court, civil case No. 3-1127/2018, 24 December 2018.

[81] Juzgado de lo Mercantil nº 9 de Barcelona, sentencia nº 159/2020, de 6 de julio de 2020.

[82] Jugement du Tribunal de commerce francophone de Bruxelles, rép. 004235; A/18/00217, 30 mars 2018.

[83] Court of Holbæk, BS-13084/2018-HBK, 28 May 2018.

[84] AGCOM Order Proc. n. 177/DDA/CA - http://rlsbb.com

Rlsbb had a global SimilarWeb ranking of 13 196 and 4.5 million visits July 2022.

Rezka.ag

Stakeholders from the audiovisual industry have reported *Rezka* again for inclusion in the Watch List.

Rezka is a popular Russian-language streaming website that allegedly offers 31 000 movies and 8 800 TV series, as well as cartoons and anime. Content can be searched and filtered by genre, year, and categories.

As reported in 2020, legal action concerning this website includes blocking injunctions or orders in Belgium[86], Russia[87] and Spain[88].

Rezka.ag had a global SimilarWeb ranking of 1 226 and 61.1 million visits in July 2022.

5.4. Peer-to-peer and BitTorrent indexing websites

Peer-to-peer and BitTorrent indexing websites use the peer-to-peer file distribution technology to permit users to share content[89]. The websites act as aggregators of peer-to-peer links, which users can search for and access via the website. When a user clicks on a link, the peer-to-peer technology allows the user to download media files stored on other users' computers across the peer-to-peer network. A user in a peer-to-peer network downloads files from other users' private storage place and makes their own files available for upload to the peer-to-peer network. Users offering a file are known as 'seeders' and they share these files with other users known as 'peers'.

The users need to download a BitTorrent client, the software that will accept a torrent file and begin downloading the data associated with it.

Indexing services usually generate income from advertisements and donations from users. BitTorrent indexing sites often register multiple domain names, allegedly in order to prevent their business from being damaged if enforcement authorities seize or block one of their domain names.

As reported by stakeholders from the audiovisual and music sectors, BitTorrent indexing websites remain a major issue in 2022 and their use remains popular. According to the

---

[85] IGAC, 28/12/2015, pursuant to a Memorandum of Understanding: Análise de queixa formulada à IGAC ao abrigo da Cláusula 5ª do Memorando de Entendimento celebrado em 30 de julho de 2015.

[86] Jugement du Tribunal de commerce francophone de Bruxelles, rép. 004235; A/18/02607, 3 août 2018.

[87] Decision of the Ministry of Communications and Mass Media, 1z-7605/2019, 5 August 2019.

[88] Juzgado de lo Mercantil nº 9 de Barcelona, sentencia nº 159/2020, de 6 de julio de 2020.

[89]Research on Online Business Models Infringing Intellectual Property Rights Phase 1: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf

input from the music industry[90], 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.

The Pirate Bay - ThePirateBay.org, pirateproxy.space, thepiratebays.com

Stakeholders from the audiovisual and music industries continue reporting *The Pirate Bay* and its proxies for inclusion in this Watch List.

Available in 35 languages, *The Pirate Bay* allegedly remains one of the largest BitTorrent websites globally. It facilitates the sharing of all kinds of content (including films, books, music, TV programmes, software and videogames) in its peer-to-peer network. The hosting location of the website is kept hidden. As reported in 2020, successful legal action concerning this website includes criminal and civil sanctions against its operators as well as its blocking in a number of jurisdictions, such as Argentina[91], Australia[92], Austria[93], Belgium[94], Denmark[95], Finland[96], France[97], Greece[98], Iceland[99], India[100], Ireland[101], Italy[102], Netherlands[103], Norway[104], Portugal[105], Romania[106], Russia[107],

[90] See contribution by IFPI, at https://ec.europa.eu/eusurvey/runner/Counterfeit_Piracy_Watch_List_2022

[91] Juzgado de lo Civil 64, expte. N° 67921/2013, 11 de marzo de 2014.

[92] Federal Court of Australia, No. NSD 239 and 241 of 2016, 15 December 2016: http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca1503; and Federal Court of Australia, No. NSD 269 of 2017, 18 August 2017: http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca0965

[93] Supreme Court of Austria, No. 4 Ob 121/17y, 24 October 2017: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=df3a2cab-8dd1-4ce4-8795-9cdfffc0e919&Position=1&Abfrage=Justiz&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=False&SucheNachText=True&GZ=4Ob121%2f17y&VonDatum=&BisDatum=09.11.2017&Norm=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=JJT_20171024_OGH0002_0040OB00121_17Y0000_000

[94] Court of Appeal of Antwerpen, Section 1, No. 3399 Rep. 2011/8314, 26 September 2011: https://nurpa.be/files/20111004_BAF-Belgacom-Telenet-DNS-blocking.pdf

[95] Danish Supreme Court, Telenor v IFPI, No. 159/2009, 27 May 2010: http://www.hoejesteret.dk/hoejesteret/nyheder/Afgorelser/Documents/153-2009.pdf

[96] District Court of Helsinki, Case No. H 11/20937, 26 October 2011.

[97] Court of Appeal of Paris, Case No. 15/02735, 18 October 2016.

[98] https://opi.gr/images/epitropi/edppi_list_v6.pdf

[99] District Court of Reykjavik, Case No. E-3784/2015, 17 October 2016: https://www.heradsdomstolar.is/default.aspx?pageid=347c3bb1-8926-11e5-80c6-005056bc6a40&id=31e3ef7d-7b6f-48a7-85b6-a74cb6bfbf95

[100] High Court of Delhi at New Delhi, CS (COMM) 724/2017 & Ors., 10 April 2019: https://spicyip.com/wp-content/uploads/2019/04/UTV-v-1337x-10.04.20191.pdf

[101] High Court of Ireland, Case No. 2008 1601 P ([2009] IECH 411), 24 July 2009.

[102] Supreme Court of Cassation, Judgment no. 49437, 23 December 2009.

[103] District Court of The Hague, Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v. Ziggo BV, Case No. 365643 –KG ZA 10-573, 19 July 2010: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2010:BN1445&showbutton=true&keyword=brein+ziggo

Singapore[108], Spain[109], Sweden[110] and the United Kingdom[111]. The CJEU has also confirmed that *The Pirate Bay* infringes copyright[112]. However, the service reportedly continues operating through multiple alternative domains hosted in various countries around the world.

ThePirateBay.org had a global SimilarWeb ranking of 1 800 and 28 million visits in July 2022.

Rarbg - Rarbg.to

Stakeholders from the audiovisual and music industry continue reporting *Rarbg* for inclusion in the Watch List.

Rarbg is reportedly a popular BitTorrent website hosted in Bosnia and Herzegovina facilitating access to a wide range of content, including music, films, TV programmes, software and videogames. As reported in 2020, legal action concerning this website and its variants includes judgments or blocking orders in Australia[113], Denmark[114], Finland[115], Greece[116], India[117], Indonesia, Ireland[118], Italy[119], Singapore[120] and the United

[104] Borgating Court of Appeal, Nordic Records Norway AS v Telenor ASA, 9 February 2010.

[105] District Court of Lisbon, No 153/14.0YHLSB, 169605, 4 February 2015.

[106] Tribunalul Bucureşti, NR. 2229/2018, 5 November 2018.

[107] Moscow City Court, civil case No. 3-716/2018, 23 August 2018.

[108] High Court of the Republic of Singapore, Case No.: HC/OS 95/2018, 26 April 2018.

[109] Central Court of Administrative Litigation Madrid, N66028, 25 March 2015.

[110] Stockholm District Court, Case Name B 13301-06, and Swedish Patent and Market Court, Case No. PMT 7262-18, 15 October 2018.

[111] High Court of Justice, Chancery Division, Case No. HC11C04518 ([[2012] EWHC 268 (Ch)], 20 February 2012.

[112] See judgment of the Court on case C-610/15: http://curia.europa.eu/juris/document/document.jsf?text=&docid=191707&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2184518

[113] https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca0965

[114] Court of Frederiksberg, BS FOR-121/2015, 6 March 2015.

[115] Finnish Court Case 311/18: https://www.markkinaoikeus.fi/fi/index/paatokset/teollisjatekijanoikeudellisetasiat/teollisjatekijanoikeudellisetasiat/1529045059067.html

[116] https://opi.gr/images/epitropi/edppi_list_v6.pdf

[117] High Court of Delhi at New Delhi, CS (COMM) 724/2017 & Ors., 10 April 2019: https://spicyip.com/wp-content/uploads/2019/04/UTV-v-1337x-10.04.20191.pdf

[118] High Commercial Court, 2017 No 11701 P (2018 No. 6 COM).

[119] Italian Regulatory Authority for Communications, Decision 35/17/CSP: https://www.agcom.it/documents/10179/6926764/Delibera+35-17-CSP/40e3701c-cf12-4662-b793-8899d767e4d0?version=1.0

[120] High Court of the Republic of Singapore, Case No.: HC/OS 95/2018, 26 April 2018.

Kingdom[121].

Rarbg reportedly generates income from advertisements and a pay-per-install distribution model for potential malware[122].

Rarbg had a global SimilarWeb ranking of 783 and 43.8 million visits in July 2022.

Rutracker - Rutracker.org

Stakeholders from the audiovisual and music industry continue reporting *Rutracker* for inclusion in the Watch List.

Rutracker is a BitTorrent website that has around 2 million active torrents and 13.9 million registered users and is one of the world's most visited pirate websites. The site is hosted in Russia by a Seychelles company. Legal action concerning this site includes blocking orders in Russia[123] and Singapore[124].

Rutracker.org had a global SimilarWeb ranking of 927 and 43 million visits in July 2022.

1337x - 1337x.to

Stakeholders from the music and audiovisual industries continue reporting *1337x* and its proxies for inclusion in the Watch List. The site has several mirror sites/alternate URLs: *1337x.st, x1337x.se, 1337x.gd, 1337x.is, x1337x.ws, x1337x.eu*.

1337x is a BitTorrent website that allegedly allows users to download films, TV programmes, music, games and apps. The identification of its actual host is not possible, as the site is masked behind a reverse proxy service. As reported in 2020, legal action concerning this website includes judgment or blocking orders in Australia[125]Austria[126], Belgium[127], Denmark[128], Greece[129], India[130], Ireland[131], Italy[132], Singapore[133] and

[121] London High Court of Justice, Claim No HC/2014/ 00466, Order 10 11 14 (5), 19 November 2014.

[122] Symantec: Pay-Per-Install – The New Malware Distribution Network - https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/security-response-pay-per-install-10-en.pdf

[123] News item: https://www.themoscowtimes.com/2015/11/09/moscow-court-orders-torrents-site-rutrackerorg-blocked-for-good-a50678

[124] High Court of the Republic of Singapore, Case No.: HC/OS 95/2018, 26 April 2018.

[125] https://www.comcourts.gov.au/file/Federal/P/NSD663/2017/3787886/event/29056799/document/1018339

[126] Supreme Court of Austria, No. 4 Ob 121/17y, 24 October 2017: https://www.ris.bka.gv.at/Dokument.wxe? ResultFunctionToken=df3a2cab-8dd1-4ce4-8795-9cdfffc0e919&Position=1&Abfrage=Justiz&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=False&SucheNachText=True&GZ=4Ob121%2f17y&VonDatum=&BisDatum=09.11.2017&Norm=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=JJT_20171024_OGH0002_0040OB00121_17Y0000_000

[127] Jugement du Tribunal de commerce francophone de Bruxelles, rép. 004235; A/18/00217, 30 mars 2018.

[128] Court of Frederiksberg, 25 August 2016, BS FOR-563/2016.

[129] https://opi.gr/images/epitropi/edppi_list_v6.pdf

Spain[134]. The website obtains revenues from advertisements and Bitcoin donations.

1337x had a global SimilarWeb ranking of 514 and 66.1 million visits in July 2022.

5.5. Unlicensed download sites

Unlicensed download sites include sites offering direct downloads of the content for free or against the payment of a fee.

Sites selling the content do so at a significantly lower price than the licensed services. The appearance of these sites is sometimes that of legitimate download services, thus confusing users. For instance, they may have the official cover art and reportedly accept payments through well-known payment provider brands such as Visa, MasterCard or PayPal. Users usually create an account, add money to it and search for the content they want to download directly from the website. The prices normally vary depending on the size of the file. These sites often offer new releases as well. As these sites allegedly do not pay royalties, they have presumably lower operation costs, thus likely competing unfairly with legitimate download services and reducing sales of licensed sites.

Sites offering the download of content files for free sometimes base their business model on revenues from advertising. Others operate to provide a free repository of content, mostly publications, often accepting donations from their users.

Music Bazaar - Music-Bazaar.com and Music-Bazaar.mobi

Stakeholders from the music industry continued to report *Music Bazaar* for inclusion in this Watch List as an unlicensed pay-per-download site.

Music Bazaar allegedly engages in the unlicensed sale of music tracks online. Albums and tracks are available to purchase at significantly lower prices than their normal retail value. The purchased album remains in the user's account for a number of days and the user can download it as many times and on as many devices as necessary for no additional fee. Free content is also available on the site.

Music-Bazaar.mobi is a subdomain and a mobile version of the .com domain.

Rightholders in the music sector reported that as of mid-February 2022, *Music-Bazaar.com* automatically redirects to *songswave.com* and *Music-bazaar.mobi*

---

[130] High Court of Delhi at New Delhi, CS (COMM) 724/2017 & Ors., 10 April 2019: https://spicyip.com/wp-content/uploads/2019/04/UTV-v-1337x-10.04.20191.pdf

[131] High Commercial Court, 2017 No 11701 P (2018 No. 6 COM).

[132]Italian Regulatory Authority for Communications, Decision 110/18/CSP: https://www.agcom.it/documents/10179/10452714/Delibera+110-18-CSP/ff89e9e8-ffa2-47ee-83b4-fd8e4af97a0d?version=1.0

[133] High Court of the Republic of Singapore, Case No.: HC/OS 95/2018, 26 April 2018.

[134] Juzgado de lo Mercantil nº 1 de Barcelona, sentencia nº 22/2019.

automatically redirects to *Songswave.tel*. *Songswave.com* and *Songswave.tel* are reported to be the same site with different domain. In the same way as *Music-Bazaar*, *Songswave* offers a wide range of international music repertoire. The site claims to add "some 100 new albums" every day.

As reported in 2020, legal action concerning *Music-Bazaar* includes blocking by internet service providers in Greece[135], Denmark[136], France[137], Russia[138] and Spain[139].

Music Bazaar had a global SimilarWeb ranking of 4 160 154 and 7 300 visits in July 2022.

***Sci-hub.io* (*Sci-hub.tw; sci-hub.cc; sci-hub.ac; sci-hub.bz and others*)**

Stakeholders from the publishing industry continue reporting *Sci-hub.tw* and its mirror sites as the most problematic online actors for scientific, technical and medical (STM) and scholarly publishers.

As explained in previous editions, *Sci-hub.tw* and its operator are allegedly hosted in Russia. The site reportedly provides unauthorised access to around 55-60 million journal articles and academic papers. The site describes itself as "the first pirate website in the world to provide mass and public access to tens of millions of research papers". It also explains that it "provides access to hundreds of thousands research papers every day, effectively bypassing any paywalls and restrictions." As reported in 2020, legal action concerning this operator includes an injunction issued by United States' courts ordering the domain registries to suspend *Sci-hub.tw*'s and its mirror sites' domain names in 2015 and a judgment by the United States' district court in the Southern District of New York[140], which ruled that the site was liable for wilful infringement of copyright. *Sci-hub* has also been subject to an injunction in France[141].

Sci-hub allegedly gains unauthorised access to publishers' journal databases by using

[135]Joint hearing of actions 61937/2013 and others, 13 December 2013. See also https://opi.gr/images/epitropi/edppi_list_v6.pdf

[136] Court of Frederiksberg, 6 March 2015, BS FOR-121/2015.

[137] On 5 July 2022 the Court of Paris ordered ISPs to block access to a number of sites including music-bazaar.com together with the new domains from which the site operates – songswave.com and songstel.com following an application filed by the music industry's collecting society SCPP; Décision du 05 juillet 2022 3ème chambre 3ème section N° RG 22/06615 - N° Portalis 352J-W-B7G-CXEUA.

[138] The site is reported to have become unavailable in Russia.

[139] On 12 April 2021 the Central Court of Administrative- Litigation nº 10 issued an Order authorising the blocking measure requested by the Second Section of the Intellectual Property Commission regarding the following domains: www.music-bazaar.com (www.music-bazaar.net. www.music-bazaar.org. www.music-bazaar.pro and www.music-bazaar.mobi). This Order was as a result of an administrative site blocking application submitted by the music industry's local group in Spain AGEDI to the Intellectual Property Commission.

[140]Southern New York District Court, 15 civ. 4282 (RWS), 28 October 2015: https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2015cv04282/442951/53/

[141] jugement-sci-hub-mars-2019Y2mate.pdf (nextinpact.com)

compromised user credentials obtained via phishing frauds[142]. Once it gains access to the journal databases, it downloads articles, stores them on its own servers and makes them available to the requesting users, while continuing to cross-post these articles to the *Library Genesis* (see below) and its related sites. The site promotes donations from users as a means to obtain revenues.

Publishers report that *Sci-Hub* changes domain frequently in attempts to obfuscate rights owner enforcement activities.

Sci-hub.io had a global SimilarWeb ranking of 938 388 and 51 800 visits in July 2022.

Library Genesis - Libgen.onl and mirror sites

Stakeholders from the publishing industry also continue reporting websites related to the so-called Library Genesis Group for inclusion in this Watch List.

As reported in the previous edition, the Library Genesis Group has been active as a website since 2008, where it operated under *libgen.org*. Following legal action, including blocking injunctions or orders issued by the Italian Regulatory Authority for Communications (AGCOM)[143] and by courts in France[144], Greece[145], Russia[146] and the United Kingdom[147], it has shut down and reopened with different names and mirror sites over the years.

Libgen.onl is hosted in both Russia and the Netherlands. It allegedly operates a repository of pirated publications, including books, scientific, technical and medical journal articles as well as scholarly materials.

Stakeholders from the publishing industry reported that the site now has a main portal under *libgen.onl*, which provides instructions and updates and lists a series of URLs. They reportedly obtain the vast majority of the scientific, technical and medical journal articles via *Sci-hub* (see above). The site boasts: "*At Library Genesis, you can choose from more than 2.4 million non-fiction books, 80 million science magazine articles, 2.2 million fiction books, 0.4 million magazine issues, and 2 million comics strips*."

---

[142] Universities and other institutions have reported instances to the European book publishing industry whereby their students and academic personnel have been subject to phishing frauds. For instance, emails claiming that a student's library access is due to expire and the individual is required to "update" his/her login credentials through a conveniently provided link (that harvests the individual's personal, private information).

[143] Italian Regulatory Authority for Communications Decision 179/18/CSP: https://www.agcom.it/documents/10179/11173566/Delibera+179-18-CSP/635047ae-0d9a-4d7b-8de9-47c5ae235f3e?version=1.0

[144] Tribunal de Grande Instance de Paris, jugement du 7 mars 2019: https://cdn2.nextinpact.com/medias/jugement-sci-hub-mars-2019.pdf

[145] https://opi.gr/images/epitropi/edppi_list_v6.pdf

[146] News item: https://www.chemistryworld.com/news/sci-hub-blocked-in-russia-following-ruling-by-moscow-court/3009838.article

[147] https://www.footanstey.com/bulletins/2835-high-court-ruling-blocking-order-imposed-on-isps-to-tackle-ebook-piracy

Other mirror sites associated with the Library Genesis Project include: *bookfi.org, bookzz.org, bookre.org, booksc.org, book4you.org, bookos-z1.org, booksee.org, and b-ok.org*.

Sites in the LibGen group, as well as proxies are reported to remain subject of a blocking order[148].

Advertising is a source of income for the sites, which also invite users to make donations.

Libgen.onl had a global SimilarWeb ranking of 311 777 and 179 800 visits in July 2022. *Libgen.is* had a global SimilarWeb ranking of 3 549 and 11.9 million visits in July 2022.

5.6. Piracy Apps

With the increase in the number of users accessing content on mobile hand devices, a whole new ecosystem of piracy apps has emerged where users move from browser-based piracy to app-based piracy using mobile devices. Generally, they are on offer on a website that provides the portal through which the app can be downloaded. These apps are often a subscription-based service, tricking users into believing the legality of the underlying service. Once downloaded and/or registered/subscribed, these apps provide users access to myriad pirate music, movie and television titles. Sometimes the apps are available in the normal store (Google Play and App Store) as they announce they offer legitimate services. A big number of apps have been reported by the audiovisual sector, including sports events organisers, as well as music sector which has reported the trend that stream ripping sites offer and promote apps on their sites for users to download. These services may require further attention in the future.

IPTV Smarters

Stakeholders from the audiovisual sector reported *IPTV Smarters* for inclusion in the Watch List as an IPTV turnkey solution from India. It is reported to be an IPTV software solution, which trades under the brand name WHMCS Smarters and offers website design and development, customised apps on several platforms and a billing platform. The operators also offer an IPTV media player through the IPTV Smarters Pro APP.

The website *iptvsmarters.com* had a global SimilarWeb ranking of 45 162 and 1.2 million visits in July 2022.

EVPAD (ievpad.com)

Stakeholders from the audiovisual sector reported *Evpad* for inclusion in the Watch List as an Android app from China that incorporates P2P technology as well as EVPAD-branded apps to enable access to more than 2 000 movies and TV titles and over 1 000 live international channels. It operates through a network of online and physical resellers around the world. It is reported to regularly launch new product lines, including a new

[148] Netzsperre: Was bedeutet "Diese Seite ist gesperrt"? (magenta.at)

brand, “EVBOX,” targeting among others also European customers. As reported by a stakeholder, a blocking injunction has been obtained against the service in Singapore.

According to SimilarWeb, *Evpad.com* had a global ranking of 350 752 and 125 200 visits in July 2022.

Shabakaty

Stakeholders from the audiovisual sector reported Shabakaty as a suite of apps developed by Iraq’s largest ISP, Earthlink. Marketed via *Shabakaty.com*, the Shabakaty apps are reported to offer unauthorised access to a bundle of pirate TV, movie, and music content from a range of copyright holders pirated television channels, alongside an on-demand service. It is available on a set-top-box, mobile app and website.

According to SimilarWeb, *Shabakaty.com* had a global ranking of 12 834 and 6.2 million visits in July 2022.

5.7. Hosting providers , including dedicated server providers

Pirate sites often depend on hosting providers, including dedicated server providers (DSPs), that provide the necessary infrastructure for them to operate (for instance easy access or fast download).

The term ‘hosting providers’ can cover a broad range of hosting services which can for example be distinguished by the type of IT resources made available to clients, and the degree to which these providers manage the services necessary to make a content available on the Internet, with the exception of managing the content itself.

IT resource needs may vary depending, among others, on the type of content distributed. In some cases, the computing power of a physical server can be shared between several clients and their websites, and the hosting provider manages the server. In other cases, like for example streaming of audiovisual content to a large public, physical servers may need to be fully dedicated to this task for performance reasons.

DSPs make such physical servers available to clients, including network connectivity. Clients can either manage their dedicated servers completely on their own, or choose a DSP which offers server management services (such management services can also be offered by third-party providers). Some hosting providers have policies against infringers and regularly take action to prevent pirate sites from using their services for copyright infringements. However, others do not follow due diligence to prevent websites from using their services for illegal activities. Likewise, some hosting providers do not cooperate with copyright holders in removing or blocking access to pirate content. A significant number of hosting providers and dedicated server providers has been reported by stakeholders. A number of the services mentioned below are reported by stakeholders to openly advertise that they will not respond to take down requests from content owners. The possibility of assessing the popularity of these services is limited and therefore no figures on ranking and visits are provided.

DDoS-Guard.net

DDoS-Guard.net (also reported to operate as *Cognitive Cloud L.P.*) is reported by audiovisual sector for inclusion in the Watch List as a 'bulletproof' hosting provider for pirate sites. Many piracy sites including s.to and bs.to are reported to be relying on Ddos-Guard's services for hosting. Rightholders report the service as not responding to takedown notices.

Private Layer

Stakeholders from the audiovisual industry continue reporting *Private Layer* for inclusion in this Watch List.

Private Layer is a company registered in Panama with servers in Switzerland. Private Layer allegedly provides anonymity to the owners and operators of the websites that use its services. It reportedly hosts infringing sites and refuses to respond to outreach notices from rightholders.

A number of **dedicated server providers** have been reported by the audiovisual sector, notably the sports events organisers, as not responding to take down requests and not taking any action to avoid infringements of copyright.

***Amarutu Technology Ltd ("Amarutu"**, also known as Koddos)*

Amarutu is reported to be a DSP, which claims to have office locations in Hong Kong (China) and Seychelles. It is reported by rightholders to consistently ignore their takedown notices.

AS-Istqservers / Istqserverses ("Istq")

Istq is reported to be a Jordanian DSP that operates multiple ASNs[149]. It is reported by rightholders as failing to take any meaningful action upon receipt of takedown notices.

HostPalace Web Solution PVT LTD ("Host Palace")

Host Palace is reported by stakeholders to be an Indian DSP, which does not to take any action to cease copyright infringements.

5.8. Unlicensed IPTV services

As explained in the previous Watch List, unlicensed IPTV services offer without authorisation access via streaming to hundreds or even thousands of TV channels illegally sourced from legitimate service providers worldwide. Their users have access to all kinds of TV content, including premium content, such as blockbusters and sports events. Unlicensed IPTV services usually offer video-on-demand (VoD) content, including unauthorised copies of movies and television series and even pre-releases of

[149] Autonomous System (AS) Numbers are allocated by IANA and are used by various routing protocols, see Autonomous System (AS) Numbers (iana.org)

audiovisual content.

Unlicensed operators offer the IPTV content for direct streaming on their websites or, more usually, through a mobile application. This application can be downloaded to the user's device, such as a Smart TV, tablet or smartphone. It can also be downloaded to a consumer device (i.e. a receiver) subsequently connected to a TV set to enable it to stream the content. Moreover, stakeholders report that some consumer devices are sold with one or more pre-installed pirate IPTV applications.

The business model of unlicensed IPTV services is usually based on subscriptions. Many consumers may actually be unaware that these Pay-TV services are illegal. Some unlicensed IPTV services also base their business models on advertising.

Stakeholders report that monitoring the activities of unlicensed IPTV services is particularly difficult. As explained in the section on piracy apps above, some unlicensed IPTV services sell their apps in "unofficial" app stores or websites[150], which do not have a procedure in place to notify apps that infringe copyright. Others invite their users to download generic apps (i.e. generic video players, not illegal as such) and explain to them how to use those apps to stream the infringing content that the unlicensed IPTV services provide[151]. In addition, the technical infrastructure related to these services is very complex, making the identification of content sources and illegal service operators challenging. For instance, stakeholders report that different actors include operators who copy the broadcasters' content and others who acquire and aggregate that content to sell it to other operators. The next link is the unlicensed IPTV service re-selling or re-streaming the bundle of channels to the end-user. This complex network of copying, re-selling, exchanging and re-streaming broadcasters' content constitutes a parallel black market that explains the multiplication of a single stream of a TV channel, eventually available not only in hundreds of unlicensed IPTV services but also in illegal streaming websites and online content-sharing service providers. Moreover, this complex network is the result of cooperation of illegal operators from various countries, making it difficult to find out the identity and precise location of an IPTV operator.

Stakeholders also reported IPTV playlist forums as contributors to sharing illicit content. These online forum sites are dedicated to or hosting a dedicated group/sub-forum to the sharing of free IPTV playlists. Forums are organised by the type of content or TV group. No specific forums are mentioned in the current Watch List but they may require further monitoring in the future.

Stakeholders from the audiovisual and broadcasting industries have reported the websites below for inclusion in the Watch List. They allegedly sell subscriptions for unlicensed IPTV services. Data on the popularity of these websites is difficult to gather. The SimilarWeb ranking of use of the websites is less relevant than in other services mentioned in this Watch List, as users may only visit the site to purchase a subscription.

[150] I.e. not in Google Play, Apple Store, or other mainstream app stores.

[151] Stakeholders from the audiovisual and broadcasting sectors have reported some of these generic applications for inclusion in this Watch List. However, none of them is listed in this document, as the evidence provided shows that they are mere video players, even if they are used by some unlicensed IPTV operators to infringe copyright.

BIPTV.best** and **BestBuyIPTV.store

BestBuyIPTV is reported by stakeholders from the audiovisual sector as operating from Vietnam and as very popular in Europe. It is reported to offer country-specific channel lists, with more than 10 000 channels from 38 countries, and 19 000 VOD titles in multiple languages. *BestBuyIPTV* is available on several platforms and operating systems. It uses resellers with different pricings. *BestBuyIPTV* advertises that it provides services to over 900 000 users, 12 000 resellers, and 2 000 re-streamers worldwide.

According to SimilarWeb, *BIPTV.best* had a global ranking of 5 336 973 and 5 200 visits in July 2022.

King365tv.com** / **Theking365tv.pro

King365tv has again been reported by the stakeholders from the audiovisual sector for inclusion in the Watch List. It reportedly operates from Algeria and gives access to over 2 200 international channels and an extensive VoD library.

According to SimilarWeb, *King365tv.com* had a global ranking of 3 328 447 and 6 800 visits in July 2022. The actual subscriber audience of this service is however believed by stakeholders to be significantly higher than the SimilarWeb data would suggest due to the fact that once a user has purchased a subscription, the user accesses the infringing content on third-party media players, and this access is not counted by SimilarWeb.

VolkaIPTV.com

VolkaIPTV.com is also reported again by stakeholders for inclusion in the Watch List. It reportedly operates from Algeria or Morocco and offers a reseller programme and customer plans of various IPTV services that provide access to about 7 500 international TV channels, as well as 17 000 films and 1 000 TV series, at low monthly subscription fees. Its estimated audience is 60 000 users.

5.9. Social media

Social media platforms enable end-users to communicate online and share content on different privacy levels (public, semi-public, private), primarily for private but also for commercial purposes. Stakeholders generally acknowledge that the social media platforms that they reported did not have as the main or one of the main purposes to infringe copyright. Nor do they seem to base their business models on activities that infringe copyright. However, stakeholders report that groups in social media are increasingly used to share copyright-protected content without authorisation. Due to the popularity of these groups, tens of thousands of users have access to this illegal content. Some social media users also use their individual accounts to offer or promote illegal services, including IPTV services.

The contributions received for this Watch List suggest that with social media penetrating more and more areas of life, possible infringements extend to the realm of e-commerce in the promotion, selling of and facilitating access to counterfeit goods across different

communication channels. The alleged misuse primarily consists of directing unsuspecting users attracted by official brand images or guided by other users or content providers, including so-called influencers (via links or otherwise) to third-party websites or cloud storage services where content can be streamed or downloaded, or counterfeits are offered for sale. This trend has also been outlined in the EUIPO discussion paper[152] about the evolving nature of social media services in infringing IP rights. According to this paper, infringers are able to reach a broad range of consumers by means of sponsored advertisements and direct them to external websites offering counterfeit products or IPR-infringing content. Advertisements of well-known brands on websites and mobile apps lead consumers to believe they acquire legally published content or original goods or services, thereby damaging the brands' reputations as well. Furthermore, information on where and how to access IPR infringing content and goods may be shared amongst users in invite-only groups or otherwise, followed-up by private messages. This may also circumvent IP protection measures and poses challenges to tracing infringing activities. This difficulty, also with regard to the sheer volume of traffic, is apparent from the EUIPO report on *Monitoring and analysing social media in relation to IP infringement* from 2021[153] demonstrating that social media platforms are tools for recurrent IPR infringements for digital content and physical products[154]. In addition, integrative and constantly changing functions of social media platforms, coupled with their global use across borders, make it difficult to navigate for IP rightholders and enforcement authorities.

This Watch List includes one social media platform, mentioned already in the last Watch List. It is not reported as having engaged in unauthorised activities, but for the reason that it is allegedly lagging behind in its efforts to combat piracy or counterfeiting.

With the diversification of social media and emerging new services further analysis and input is needed in the future for a more comprehensive approach.

VK.com (V Kontakte)

Stakeholders from different sectors representing brand owners and audiovisual industries continue to report *VK.com* for inclusion in this Watch List.

VK.*com* is a social network based in Russia but available in many languages, including English. It is the leading social network in Russia and Russian speaking territories.

[152] EUIPO, *Social media – Discussion Paper, New and existing trends in using social media for IP infringements activities and good practices to address them*, 2021 - https://euipo.europa.eu/ohimportal/fr/news?p_p_id=csnews_WAR_csnewsportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=2&journalId=8749866&journalRelatedId=manual/

[153] https://op.europa.eu/en/publication-detail/-/publication/0f9b68ae-b138-11eb-8307-01aa75ed71a1/language-en

[154] It may be exemplified by conversations related to different product categories for which social media may be misemployed as search engines for content and products, such as counterfeit medicines (pharma related conversations suspected of referring to counterfeit medicines peaking twice depending on the lockdown measures back in 2020).

Rightholders report that *VK.com* users can have unauthorised access to films and TV shows, including via embedded video players. This occurs in groups where users can share, upload and download content. A search function makes it relatively easy for users to find the infringing content. Other stakeholders report a significant number of counterfeits in their service.

Some stakeholders acknowledge that *VK.com* has taken steps to limit access to third party applications dedicated to downloading content from the site and to block infringing sites from accessing videos stored on *VK.com.* They also claim that *VK.com* has a dedicated tool for rightholders to report infringements. However, *VK.com* is included again in this Watch List because stakeholders report a high number of infringing files available on the site, variable response against reported infringements and lack of action to prevent further infringements.

In 2020 *VK.com* responded to the allegations made by other stakeholders and reported on new measures to avoid the availability of unauthorised content in their site. For instance, they notify their users of the need to respect copyright not only in the terms and conditions of the site but also before every upload of a file. *VK.com* also informed that they had in place a special procedure for removal of unlicensed content that rightholders may report by filling out an online form. *VK.com* reported that they had handled more than 1.36 million claims, the vast majority of which ended up in content removal, with a response time of less than 24 hours. Moreover, *VK.com* informed that they had put in place content identification technologies to prevent the availability of unauthorised content in their service. Finally, *VK.com* reported that a lot of content available in the service had been uploaded by the rightholders or was subject to licences concluded between *VK.com* and other service providers, including Russian television networks and streaming providers. No new information was provided for the purposes of this edition of the Watch List.

VK.com had a global SimilarWeb ranking of 16 in July 2022 and 4 in Russia. It had 4 billion visits in July 2022.

5.10. Piracy Supporting Services

A new type of service supporting piracy has been reported by the stakeholders, designated as 'Piracy-as-a-Service'. As explained by the stakeholders, these services provide a suite of off-the-shelf services that make it easy for would-be pirates to create, operate, and monetise a fully functioning pirate operation. They are reported to include, for example, website templates that facilitate setup of streaming websites; databases providing access to tens of thousands of infringing movies and TV series, in exchange for payment of a fee or a cut of the advertising revenue; dashboards that allow an illegal IPTV operator to oversee the infrastructure of their service, hosting providers that provide a safe haven for pirates, video hosting services that obscure links to infringing content and decentralised streaming software that acts as a third party tool between a streaming site and a cyberlocker or video host, allowing for quicker upload of content with a large variety of cyberlockers and video hosting services.

2embed.ru

2embed.ru has been reported by stakeholders in the audiovisual sector as a pirate content management system (CMS) library used by at least 30 sites. The site's CMS is reported

to crawl various websites and search engines to find movie and TV show streaming links which are then stored in their database and served through their API (Application Programming Interface) service. It offers a large library of movies via streaming, direct link, or embedding. *2embed* provides its service for free and remunerates itself by inserting ads.

2embed.ru had a global SimilarWeb ranking of 75 329 and 1.1 million visits in July 2022.

Fembed.com

Fembed.com, reported to be operated from Vietnam, has been reported by stakeholders in the audiovisual sector. *Fembed* is a CMS service that is reported to be commonly used by pirate movie streaming websites. *Fembed* generates revenue either from advertising – by inserting ads in *Fembed*'s media players embedded in its customers' illegal streaming services – or by charging a premium fee that allows its customers to generate revenue by inserting their own ads.

Fembed.com had a global SimilarWeb ranking of 25 266 and 3.3 million visits in July 2022[155].

6. E-COMMERCE PLATFORMS

E-commerce platforms increase consumers' choice and their feeling of comfort and safety, but at the same time they may also attract merchants who seek to deceive online shoppers and distribute counterfeit goods. Consumers may be led to believe that the product they buy is genuine, only to discover a counterfeit delivered to their homes. As indicated above, the study on *Risk and Damages Posed by IPR Infringement in Europe* from June 2021, which relies on the earlier study[156], highlights that 70% of Europeans shopped online in 2020, according to Eurostat. Consumers find it difficult to distinguish between genuine and fake goods, especially online; on average nearly 9% of Europeans claimed that they were misled into buying counterfeits.

The sale of counterfeit goods over the internet presents a threat considering that: (i) consumers are at a growing risk of buying sub-standard and possibly dangerous goods, (ii) the brand image and economic interests of EU companies are damaged through the sale of counterfeit versions of their products, and (iii) the efforts of e-commerce platforms to be regarded as safe places to purchase legitimate products are undermined.

The Commission has stepped up efforts to tackle this threat through different measures, including the *Recommendation on measures to effectively tackle illegal content online*[157], published on 1 March 2018 and the recently adopted Digital Services Act ("DSA") referred to above.

---

[155] SimilarWeb numbers only reflect end-user traffic that comes directly to its site and not the traffic that passes through its CMS customers that operate their own streaming services.

[156] EUIPO-OECD Study on *Trade in fakes in small parcels* - https://euipo.europa.eu/ohimportal/fr/web/observatory/trade-in-fakes-in-small-parcels

[157] Commission's *Recommendation on measures to effectively tackle ilegal content online* - https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

The Recommendation outlined certain principles and safeguards that should guide the activities of the Member States and of the service providers in identifying, preventing reappearance of and removing illegal content.

The Recommendation identified best practices, which online platforms were encouraged to follow in order to reduce the availability of illegal content, including counterfeit offers on e-commerce websites. The Recommendation aimed in particular at clearer notice and action procedures, more effective tools and proactive measures to detect and remove counterfeit listings and other illegal content, more transparency on online platforms and closer cooperation with trusted flaggers, rightholders and enforcement authorities.

The Digital Services Act, provides further detailed rules on online marketplaces, such as rules on notice and action and flagging of illegal content, new obligations on traceability of business users in online market places to help identify sellers of illegal goods or reasonable efforts by online marketplaces to randomly check whether products or services have been identified as being illegal in any official database, greater transparency on actions taken and obligations for very large platforms to prevent the misuse of their systems by taking risk-based action and by independent audits of their risk management systems.

In the course of the public consultation, stakeholders, while acknowledging that e-commerce platforms do not infringe IPR directly or base their business models on activities that infringe IPR, reported that certain e-commerce platforms did not take appropriate steps to tackle offers of counterfeit goods made by sellers who use these platforms. During the public consultation for the preparation of this Watch List, the following main criteria for the selection of e-commerce platforms to be included in the Watch List were identified: the estimated amount of counterfeit goods offered on their platforms, the alleged low effectiveness of the measures to detect and remove counterfeit offers and/or the alleged insufficient level of cooperation with rightholders and enforcement authorities. Other factors reported such as the lack of clarity of the platforms' terms of service regarding prohibiting their use to sell or otherwise trade in counterfeit goods and services, the absence of effective vetting of the sellers who are trading on the platforms, or absence of repeat infringer policies were considered.

The section on e-commerce platforms draws a difference between e-commerce platforms that have been reported by stakeholders but which are deemed to have demonstrated that they take sufficient measures to fight piracy and counterfeiting and e-commerce platforms that are lacking in measures or need still to go through significant improvements.

Ongoing efforts to reduce the offer of counterfeit goods

During the public consultation, a number of stakeholders nominated also this year platforms operated by Alibaba (*Aliexpress.com*, *Tmall.com*, *Taobao.com*, *1688.com*) Amazon *(Amazon.com*) as well as Meta (Facebook), which according to them still have an important number of counterfeit goods on offer. At the same time, the measures taken by these platforms in light of compliance with the *Recommendations on measures to effectively tackle illegal content online* remain higher than that of the below listed e-commerce platforms. They have reported on a range of measures to prevent and filter counterfeit offers and have been cooperating with rightholders, including as signatories of

the *Memorandum of Understanding on the sale of counterfeit goods via the internet*[158], as well as with law enforcement authorities.

Amazon and *Alibaba* attend awareness-raising and other meetings organised by Europol. *Amazon* has created an online IPR investigation team ('Counterfeit Crime Unit') to enhance the cooperation with rightholders, national law enforcement authorities, and Europol (e.g. by identifying any potential cases where Europol could be involved). Taking into consideration the engagement of these operators in the fight against counterfeiting, these platforms are not listed in this Watch List even if there is room for further improvements and they need to continue cooperating further with rightholders and law enforcement authorities.

The EUIPO has also been working with a number of e-commerce marketplaces that are making their services available to users in the EU to gather information on their IP protection tools. The objective is to make it easier for IP rightholders in general, and SMEs in particular, to take action in case they discover a potentially infringing or counterfeit version of their products for sale on such marketplaces. Depending on the IP protection tools of the participating marketplaces, this may include information on and useful links to their notification systems, IP protection programmes and contact points. To date the EUIPO has gathered information from 14 e-commerce marketplaces that is made available in the EUIPO Users' area, as well as on the website of the EUIPO Observatory on Infringements of IP Rights[159]. As a next step, the EUIPO is working with a number of IP rightholders and e-commerce marketplaces, to grant marketplaces access to new IP Enforcement Portal[160] dedicated functionalities, starting with the possibility for e-commerce marketplaces to use IPEP to verify IP rights, and get points of contacts from participating rightholders.

Some e-commerce platforms listed in the previous edition have provided new information on the measures taken and shown further commitment to improve their actions to fight piracy and counterfeiting. These additional efforts may take time to give concrete results in the reduction of piracy and counterfeiting and will therefore require further monitoring to confirm their actual deployment and efficiency, but in order to acknowledge their efforts and engagement, they are presented below in a separate section.

E-commerce platforms, which have made progress but need further monitoring

Shopee

Stakeholders from different sectors, such as the electronics, fashion, toys, luxury, reported *Shopee* again for inclusion in the Watch List. *Shopee* is one of the biggest business-to-consumers online e-commerce platforms in Southeast Asia, present on 13 markets, with its headquarters in Singapore. It allegedly sells a high volume of counterfeit goods in Southeast Asia.

[158] See footnote 51

[159] Protecting your IP rights on e-commerce marketplaces - Observatory (europa.eu)

[160] IP Enforcement Portal - Observatory (europa.eu)

Stakeholders have reported the marketplaces operated by *Shopee* mainly because of lack of proactive measures, burdensome notices system, slow removals of infringing listings and lack of common policies of enforcement, as well as limited cooperation with rightholders.

In response to the allegations made by other stakeholders, *Shopee* has reported that it has started to take a number of actions since last year to enhance their measures, notably a new IP Brand Protection Portal that is being rolled out and allows to file notices centrally for all its marketplaces. They have also indicated plans for coming months to provide for a clearer user policy, strengthening the sellers vetting and education activities and developing new tools for proactive monitoring based on new technologies. *Shopee* has also reported on its commitment to reduce the compliant handling time to seven days and increasing cooperation with right owners and their associations, as well as law enforcement.

Dhgate

Stakeholders from the different sectors, such as fashion, luxury, jewellery, and sport industries have again reported *Dhgate* for inclusion in the Watch List. *Dhgate* is the largest business-to-business e-commerce platform in China, allegedly selling high volume of counterfeit goods. .

Stakeholders have reported this platform mainly because of the alleged inefficiency of its policy to vet sellers, to use proactive measures to detect illegal listings, for the inconsistent and burdensome requirements in relation to information required to support enforcement and for the failure to efficiently apply and enforce sanctions against repeat infringers.

Stakeholders acknowledge that certain improvements have been implemented over the past years, including further cooperation with rightholders, but considered that these remain insufficient to significantly decrease the number of counterfeits on this platform.

In response to the allegations made by other stakeholders, Dhgate has reported further measures taken in the first half of 2022 and planned activities for the second half of 2022. They reported to have developed technology for proactive measures, increased cooperation with rightholders, further strengthened their seller verification system. As plans for further improvements, they reported their intention to expand the elements considered for seller identification and building a seller localisation system, upgrading their terms of use, including repeat infringer policy. They also reported their intention to publish an annual report on enforcement activities.

Other e-commerce platforms

Tiu.ru, Deal.by** and **Satu.kz

Stakeholders representing brands across sectors, such as fashion, luxury, sports, toys, tobacco, alcohol, entertainment, health and beauty sectors continue reporting Tiu.ru (Russia) Deal.by (Belarus) and Satu.kz (Kazakhstan). The most important one is Tiu.ru,

which is among the largest business-to-consumers marketplaces in Russia allegedly selling a high volume of counterfeit goods.

The marketplaces were nominated mainly because of a cumbersome takedown procedure, which includes overly burdensome administrative requirements, the overly long processing time to handle complaints, the lack of proactive measures and repeat infringers policy, as well as lack of cooperation with rightholders.

Tokopedia

Stakeholders from a variety of sectors, including footwear, apparel and equipment cosmetics, fashion, food, luxury, sport and toy sectors reported *Tokopedia* again for inclusion in the Watch List. *Tokopedia* is one of the most popular business-to-consumers and business-to-business online e-commerce platforms in Indonesia, selling a high volume of allegedly counterfeit goods.

Stakeholders have reported this marketplace mainly because of the ineffectiveness of the proactive measures to detect and filter counterfeit offers, the cumbersome take-down procedure and slow response time. Stakeholders have reported at the same time that Tokopedia has introduced a Brand Alliances program to provide better collaboration and proactive measures to reduce counterfeiting activities on the platform, which however is limited to brands with official stores on the platform.

In response to the allegations made by other stakeholders, *Tokopedia* has reported in 2020 that it strictly prohibits the sales of IPR-infringing goods and content on its platform. *Tokopedia* has in place a notice and takedown procedure to enable brand owners and customers to notify, among others, IPR-infringing offers on the platform and has shown openness to improve its procedures further. No new information was provided by *Tokopedia* for this edition of the Watch List.

7. ONLINE PHARMACIES AND SERVICE PROVIDERS FACILITATING THE SALES OF MEDICINES

Following the 2020 joint study on *Trade in counterfeit pharmaceutical products*[161], the EUIPO and the OECD reported on *Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks*[162]. This study details quantitative information on the value of the illicit trade in fake goods that can pose health risks (e.g. fake pharmaceuticals or food products), safety risks (e.g. counterfeit automotive spare parts, fake batteries) and environmental risks (e.g. fake chemicals or pesticides). The most commonly traded product categories of dangerous fakes were perfumery and cosmetics, clothing, toys, automotive spare parts and pharmaceuticals. Most of these goods originated in China (55% of global customs seizures) and Hong Kong (China)

[161] https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade_in_Counterfeit_Pharmaceutical_Products/Trade_in_Counterfeit_Pharmaceutical_Products_en.pdf

[162] OECD/EUIPO (2022), Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks, Illicit Trade, OECD Publishing, Paris, https://doi.org/10.1787/117e352b-en

(19%). In addition to Asian countries, in respect of global seizures, Türkiye (9%) was also an important provider of dangerous fake products. Due to its geographical location, Türkiye is a more important supplier of dangerous counterfeit goods in Europe than worldwide. The report *EU enforcement of intellectual property rights: results at the EU border and in the EU internal market, 2020*[163] by the Commission and the EUIPO indicated as main countries of provenance for medical products (medicines and other products (condoms)) Türkiye with 58.1%, China with 36.21% and Vietnam with 1.91% of articles.

For regions with vulnerable medical supply chains and for which the products' integrity is not assured throughout the entire process, counterfeit medicine may easily penetrate the ordinary public health sector. The various risks associated with substandard counterfeit medicine can therefore affect patients not even being aware of its illicit origin, increasing mortality, morbidity and the prevalence of disease such as pneumonia or malaria[164]. Moreover, in countries with marketing rules for medicines that are less stringent than in the EU, these products may be marketed outside specific marketing channels via e-commerce platforms, either directly to consumers or from business to business.

Patients in the EU can rely on receiving original medicine when choosing legitimate suppliers, including from online retailers registered with the national competent authorities in the EU Member States, identified by a common logo that appears on the websites of these registered retailers[165]. However, some consumers may also turn to bogus online markets or social media to order counterfeits.

In fact, according to the *IP Crime Threat Assessment 2022*[166] by EUIPO and Europol, the trade in counterfeit pharmaceutical products in the EU has been increasing over recent years, with medicines appearing as the seventh most-seized products at the EU's external border in 2020. Whilst most trading activity is believed to take place on the surface web, some pharmaceutical products are also distributed via dark web platforms. Counterfeit pharmaceuticals are widely advertised and offered for sale on social media platforms, facilitated by prepaid credit card and cryptocurrency payments. Seized illicit counterfeits cover a wide range of medicines including anti-cancer drugs, analgesics, antioestrogens, antivirals, antihistamines, anxiolytics and psychiatric drugs, erectile dysfunction medicines, anabolic substances, metabolic regulators, and self-testing kits for HIV and other infections.

The majority of illicit online pharmacies employ the top-level domain .com to avoid raising any suspicion, as well as .net or .org. In addition, specific terms attracting potential buyers such as 'genuine', 'discounted', 'generic', 'pharmacy', 'tablets' or the names of the genuine medicines are used on the website. In general, the websites are in English but in respect of the product names, the language is often adapted to the specific

[163] 2021_Joint_TAXUD_EUIPO_document_on_detentions_during_2020_FullR_en.docx (europa.eu)

[164] According to an WHO estimate, as cited in the Dangerous Fakes report referred to above, between 72 000 and 169 000 children may die from pneumonia every year after receiving counterfeit drugs, and fake anti-malarial medication might be responsible for an additional 116 000 deaths.

[165] Buying medicines online | European Medicines Agency (europa.eu)

[166] Intellectual Property Crime Threat Assessment 2022 | Europol (europa.eu)

country concerned. All common payment options are usually accepted (e.g. PayPal, credit cards, bank transfers).

The report on *IP Crime and its Link to other Serious Crimes (Focus on Poly-Criminality)*[167] by Europol and EUIPO also showed that the main criminal activity related to counterfeit pharmaceuticals is usually linked to other offences committed by organised crime groups. According to investigations, these concern: drugs and illicit substances, crimes against the public health, money laundering, fraud, bribery, document fraud and corruption.

The global trafficking of counterfeit medicines marketed and sold online is combatted by a number of global and regional initiatives such as the Operation Pangea carried out by INTERPOL, which in 2021 removed 113 020 websites, the highest number since the first operation in 2008[168]. A regional pan-African police operation jointly coordinated by INTERPOL and AFRIPOL conducted inspections at roadblocks, open markets, pharmacies, warehouses and other locations suspected of producing, smuggling, storing or distributing fake pharmaceuticals. It resulted, amongst others, in a seizure of more than 300 000 epilepsy tablets in Niger[169].

According to the European pharmaceutical industry, safe haven domain name registrars continue to play a major role in the ecosystem to market counterfeit medicines, acting contrary to their registrar accreditation agreements in serving rogue online pharmacy networks.

As in the realm of e-commerce platforms, experts have commenced to identify a number of good practices to prevent the IP-infringing use of a domain in each stage of its life cycle, as discussed in the *DOMAIN NAMES – DISCUSSION PAPER Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities* by the EUIPO[170]. Such good practices on the part of domain name registrars may entail the clear listing of an IPR infringement as a breach of contract leading to the suspension of a domain. Mechanisms should be put in place to allow the verification of the identity of the registrants. Some domain name registrars have already developed systems to automatically detect abusive domain registration applications and suspend them. After the registration of a domain, notice and takedown processes should be available to notify domains with illegal content, developed in cooperation with public or law enforcement authorities.

8. PHYSICAL MARKETPLACES

Stakeholders from different industry sectors reported a high number physical marketplaces located around the globe. The majority of goods concerned are consumer

[167] EUROPOL-EUIPO Polycriminality Report 2.docx (europa.eu)

[168] Pharmaceutical crime operations (interpol.int)

[169] Pharmaceutical crime: first INTERPOL-AFRIPOL front-line operation sees arrests and seizures across Africa

[170] 2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf (europa.eu)

items such as clothing, fashion accessories, eyewear, perfumes, bags and suitcases, watches, electrical appliances, stationary items and toys, offered mostly in shopping malls or bazar-type open markets. For consumers frequenting these markets it may not be evident that these goods are counterfeits and they are therefore not aware of possibly associated health and safety risks.

The selection of the marketplaces for the following listing is based on various criteria to identify those which are likely to cause harm for IP rightholders from the EU. Marketplaces reported by a variety of stakeholders corroborated by verifiable information are more likely to feature on the list. Together with the estimated size and volume of sales, the level of overt IPR infringements and the share of displayed IPR infringing goods was also considered. In this context, information provided on actions taken to curb the availability of IPR infringing goods is reflected in the listing below as well given that the Watch List is intended to encourage further measures by the market operators, as well as by local enforcement authorities.

The listing of physical markets remains illustrative and is presented in an alphabetical order by countries where they are located. In certain regions physical markets offering counterfeit goods are widespread across borders. The fact that physical markets are listed for one country, whereas no market is listed for a neighbouring country, does not imply that significant IPR infringements do not occur in markets of the latter. For Latin America, for instance, in addition to the markets in the countries listed below, stakeholders have reported on numerous marketplaces in Bolivia, Paraguay, Uruguay and Peru, albeit providing little information other than the location and the type of goods sold. Furthermore, stakeholders may no longer notify certain marketplaces despite their possible continuous operation.

For marketplaces comprehensively described in the previous editions of the Watch List, this edition provides less information, without prejudice to the actual significance of these markets. In any event, to the extent reported by stakeholders in the public consultation, the Commission services will also use the information provided on marketplaces not listed, notably in the framework of their cooperation with EU's trading partners, such as IP dialogues, working groups, as well as technical cooperation activities.

Argentina

La Salada with its sub-markets in Buenos Aires and *La Salada de Mendoza*, located in Santa Rosa (Mendoza Province), continue to be listed by several stakeholders as one of the biggest (wholesale) marketplaces of counterfeits in Argentina and beyond, as previously described. The two former Watch Lists referred to conducted raids including the arrest of the suspected market leader but the alleged massive amount of available counterfeit goods persists.

Another example of the reported markets is the *Once Neighbourhood* in Buenos Aires. Stakeholders recognise successful actions taken by public authorities in the past but sellers of counterfeits have allegedly returned.

Bosnia and Herzegovina

Stakeholders referred to the *Arizona* market, a vast informal market in Brčko close to Croatia with alleged cross-border supply chains and wholesale activities for a wide range

of counterfeit goods. According to stakeholders, parts of the goods are delivered unbranded to the market, where the respective trademarks are then affixed to the goods before they are being offered for sale. Raids are purportedly difficult to initiate due to the local authorities' complex division of administrative responsibilities.

Brazil

The markets in the *Rua 25 de Março* area of São Paulo allegedly continue to constitute the epicentre of wholesale and retail activities for counterfeits in Brazil. Enforcement operations as referred to in the previous Watch List are reiterated and show some signs of success. At the beginning of 2022, for instance, an operation involving public authorities, as well as rightholders, resulted in the confiscation of nearly 4 tons of toys at a shopping mall in Barão de Duprat Street. Furthermore, the authorities destroyed 40 tons of watches, which had been seized back in 2019 during a raid in São Paulo. Nevertheless, the mere confiscation of millions of goods in recent years and temporary closures of shops do not seem to diminish the overt IP violations.

Stakeholders also inform about initiatives such as the launch of a label for shops free of counterfeit goods in the Brás area, which still need to bear fruits to reduce the illicit sale of goods.

Nova Serrana in Minas Gerais State is reported as a major production site for counterfeit sport shoes, distributed in Brazil and other Latin American countries, as well as for household goods such as detergent powder. Enforcement actions against manufacturers and distributors have been conducted upon requests by IP rightholders, resulting in some production facilities relocating to other cities in Minas Gerais State. However, it is claimed that the large scale production of counterfeits continues.

Stakeholders also report various marketplaces in other cities such as the *Feirão des Malhas* in Rio de Janeiro or *Feire de importados* in Brasilia.

China

Stakeholders continue to report a high number of markets across China, in total more than 50, often entirely dedicated to the sale of a wide range of counterfeits. Law enforcement authorities regularly conduct raids at many of them; however, even civil and criminal convictions of the direct infringers do not appear to affect the operation of the markets in the longer term, with offers for counterfeits becoming less blatant at best. For other markets, stakeholders complain about a lack of inspection and enforcement activities in the first place.

The COVID pandemic and China's lockdown policies have affected some of the markets previously reported, shutting them temporarily down and reducing the number of visitors, in particular of foreigners. It also restricted the means to verify the information received on the market places in the public consultation for this Watch List. In consequence, fewer market places are listed in this edition.

Markets listed in the 2020 Watch List have been reported again with descriptions as previously summarised, in particular the *Asia Pacific Xingyang Fashion and Gifts Plaza* in Shanghai, the *Anfu* market in Putian City (according to stakeholders with some sellers moving their business to sell counterfeits online) and the *Silk Market* in Beijing (allegedly

with counterfeit sales of handbags, wallets, shoes and watches becoming more visible in the past 2 years).

Colombia

The *San Andresitos* markets encompassing numerous shopping centres in different areas of Bogota (San Andresito San Jose, San Andresito de la 38, San Andresito del Norte) with thousands of stalls selling high volumes of counterfeit goods for a variety of consumer goods have been reported again by several stakeholders. Some of the shopping centres and stores also offer their goods online[171].

A stakeholder also referred to the *Palacio Nacional* in Medellín and the shops in the adjacent area nicknamed "*El Hueco*", in particular for counterfeit apparel and footwear.

India

The *Karol Bagh*, *Tank Road* and *Gaffar* markets in New Delhi continue with their retail and wholesale shops offering a wide selection of counterfeit goods despite the fact that successful civil and criminal enforcement actions have been performed, including decrees obtained from courts, permanent injunction and monetary recoveries. In the previous year, the police in New Delhi conducted for instance raids to seize fake car parts offered in several markets, such as *Karol Bagh*, but such counterfeits remain available.

Equally, stakeholders report again a number of other marketplaces across India, as referred to in the previous Watch Lists, such as the *Crawford market* and *Heera Panna market* in Mumbai, the *New Market* and *Khidderpore* in Kolkota, only some noting a marginal decrease of offers in counterfeiting goods in recent years.

Indonesia

Mangga Dua Market and *Tanah Abang Market*, both in located in Jakarta with hundreds of shops, as described in the 2018 and 2020 Watch Lists, were reported again by several stakeholders. Conducted raids, if any, remain ineffective to combat the rampant sale of counterfeit goods on retail and wholesale basis.

In addition, as in the 2020 Watch List, marketplaces in other parts of Indonesia allegedly offer counterfeits in high volumes as well, particularly in Banten and on Bali, catering for tourists.

Malaysia

The markets featuring in the previous Watch Lists, notably the *Petaling Street Market* and the *Berjaya Times Square* shopping complex in Kuala Lumpur or the *Taman Johor Jaya* market in Johor Bharu (next to Singapore) are purportedly still places with considerable offers for counterfeits, despite frequent raids initiated by rightholders in some of those markets. Many stalls have closed down during the COVID pandemic, in particular those frequented by tourists, it remains to be seen whether they resume with their offerings for counterfeits. Other markets, such as *Low Yat Plaza*, a shopping mall

[171] Sanandresito de la 38; San Andresito Colombia | La Tienda Online del los Colombianos

for IT related products, are back in operation with offers for counterfeits, such as mobile phone accessories.

Further malls reported include for instance *Plaza TAR* or *GM Plaza* in Kuala Lumpur, with mostly wholesalers offering a variety of counterfeits.

Mexico

The *El Tepito* open air market in downtown Mexico City and the *San Juan de Dios* market in Guadalajara, purportedly the largest indoor markets in Latin America, as described in the previous Watch List, have been reported again with no apparent progress to effectively curb the sale of high volume counterfeit goods on retail and wholesale basis.

Morocco

Souk Korea in Casablanca and *Marrakesh Souks* remain central open markets with vast offers for counterfeit goods. Stakeholders report that public authorities take insufficient actions, information on imminent raids is leaked and any possible raids face resistance. Endeavours to enforce IP rights in civil proceedings are allegedly futile as well.

Similar issues are noted for the *Derb Soltan Fida* market in Casablanca with its offer of sportswear.

Philippines

Baclaran and *Divisiora* markets in Manila are reported for offering a wide range of counterfeit goods on retail and wholesale basis, in particular shoes, with some stalls allegedly also running online shops offering counterfeit goods. According to stakeholders, no police actions are taken.

Shops in the *Greenhills* and *Cartimar* shopping malls and in particular the stalls located in their vicinity are reported to sell higher quality counterfeit goods. The National Bureau of Investigation referred in April 2022 to a seizure of more than EUR 1 million worth of possible counterfeit goods in the *Greenhills* shopping centre, coupled with the public pledge to take additional steps to curb down the sale of counterfeits.

Russia

The *Sadovod* shopping complex in Moscow, with supposedly 100 000 customers per day visiting thousands of stores, was listed by several stakeholders for its widespread offers of counterfeit goods, in particular clothes and shoes, on retail and wholesale basis. The evident sales of counterfeits was subject to media coverage but public authorities are reportedly reluctant to take any action despite repeated complaints from rightholders in the past.

Apart from other markets, stakeholder referred in particular to *Dubrovka* market for huge amounts of sales of counterfeit consumer items and for a lack of interventions by public authorities.

Serbia

The *Buvljak open market* in Subotica, close to the Hungarian border, was reported by stakeholders. This market is one of the largest in Serbia with hundreds of stalls openly selling a variety of counterfeits, predominately clothing and sports shoes, originating mostly from China and Türkiye but also with some supplies from local production. Raids attempts by the police were allegedly pushed back by sellers with no apparent further actions taken by public authorities.

Stakeholders also referred to a market in Novi Pazar.

Thailand

The 2018 and 2020 Watch Lists featured the *MBK Centre* shopping mall in Bangkok, with hundreds of shops often visited by tourists, many of which are dedicated to offering almost exclusively counterfeit products such as clothing, bags and sportswear. Public authorities show considerable efforts to conduct ex officio actions and cooperate closely with rightholders. However, despite regular raids and official warnings part of the sellers continue to offer counterfeits. Stakeholders claim that legal actions against the operator of the *MBK Centre* cannot be initiated, which reduces the chances of a permanent closure of all shops concerned.

Similar issues are noted for the *Patpong* night market in Bangkok.

Shops in the *Platimum* mall in Bangkok continue to offer counterfeits as well but rightholders also positively note a decrease thereof.

Other markets in cities close to the boarders with Cambodia and Myanmar were mentioned by stakeholders as well.

Türkiye

Several stakeholders referred to the *Ak Çarşı* wholesale mall for textiles and shoes in Istanbul as one of the markets with the highest volumes of sales of counterfeits, estimated at millions per year. It is claimed that public authorities take no proactive measures and the responsible operators remain unresponsive to pursuits from rightholders to tackle these issues persisting for years.

The *Grand Bazaar* in Istanbul, a major tourist attraction, as reported in previous Watch Lists, shows no apparent positive development despite a number of conducted raids and criminal prosecutions.

The *Bedesten Çarşısı* market in Izmir, selling allegedly more than 200 000 pairs of counterfeit shoes per year, was indicated by various stakeholders as well.

United Arab Emirates

The *China Mall* in Ajman, allegedly one of the biggest wholesale and retail distribution centres and transit hubs in the Middle East, was listed in the previous Watch Lists. Stakeholders inform that Ajman authorities have recently initiated a number of raids inside the mall resulting in significant seizures and in a reduced visibility of counterfeits at offer. However, more clandestine sales to trusted groups of resellers are purportedly persisting.

The *Dragon Mart* in Dubai, by its own account the world's largest Chinese mall and trading hub for Chinese products outside mainland China for retail and wholesale with more than 6 000 shops, was reported again. It allegedly provides a gateway for the supply of Chinese products in the Middle Eastern and North African markets for a wide variety of counterfeit products. Stakeholders claim that the numerous raids conducted by the Department of Economic Development agents and the police are not eradicating the sale of counterfeits due to relatively low fines against shop owners, the non-liability of the mall operator and the limited seizures of counterfeits, which are mostly stored elsewhere.

According to stakeholders, sales and trade in counterfeit products remain rife in the *Jebel Ali Free Zone* in Dubai. Stakeholders commend, however, that the Dubai Department of Economic Development, signed a Memorandum of Understanding with the Dubai Police, allowing it to take actions in this area.

Other bazars and informal markets were indicated as well. In particular, several stakeholders referred to the *Karama* shopping complex in Dubai, which despite raids conducted by the Department of Economic Development carries on to offer counterfeits such as leather goods, shoes or watches.

Vietnam

As in the previous Watch Lists, *Saigon Square Plaza* continues to operate despite regular or even frequent raids taking place, according to stakeholders. The same applies regarding the other markets formerly featuring in the Watch List, such as *Lucky Plaza* or the *Dan Sinh Market* in Ho Chi Minh City, where also automotive parts such as oil and air filters are available, or the *Dong Xuan market* in Hanoi.