EUROPEAN
COMMISSION

Brussels, 14.12.2020
SWD(2020) 360 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 right holders and 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. The COVID-19 pandemic is proving that criminals quickly adapt to the new trade environment and find their way to infiltrate the legitimate supply chain with their counterfeit and often dangerous products.

In terms of economic harm, the Organisation for European Co-operation and Development (OECD) and the European Union Intellectual Property Office (EUIPO) published in March 2019 an updated report[1] that shows that in 2016 counterfeit and pirated goods worth EUR 460 billion were traded worldwide, which represents a 3.3% share in world trade (up from 2.5% of world trade in 2013). The imports of counterfeit and pirated products into the EU amounted to as much as EUR 121 billion, which represents up to 6.8% of EU imports (up from EUR 85 billion, or 5% of total EU imports in 2013). Both figures are significantly higher than in the first edition of the study three years earlier, showing that the problem of counterfeit trade has become more serious.

The five countries in the world most affected by trade in counterfeit and pirated products are the United States, France, Italy, Switzerland and Germany[2]. The cumulated impact for all EU countries is double that for the United States[3].

The 2020 Status Report on IPR infringement[4] prepared by the European Observatory on Infringements of Intellectual Property Rights found that imports of counterfeit goods to the EU seem to be most intensive for luxury and fashion products such as leather articles and handbags, watches, perfumes and cosmetics, footwear, jewellery, and sunglasses. However, counterfeiters also target common consumer products imported into the EU, such as toys and games, footwear and clothing. In addition, counterfeit or pirated intermediary products, such as electronics goods and ICT devices or spare parts, are also frequently imported into the EU.

The sectors studied (cosmetics and personal care; clothing, footwear and accessories; sports goods; toys and games; jewellery and watches; handbags and luggage; recorded music; spirits and wine; pharmaceuticals; pesticides and agrochemicals; smartphones) generated a revenue loss up to EUR 50 billion due to counterfeiting and piracy, which is equivalent to 6.4% of EU-wide sales in these sectors. This translates into a direct loss of 416 004 jobs in these sectors across the EU and a total employment loss of 671 435 jobs.

---

[1] EUIPO-OECD Study on *Trends in Trade in Counterfeit and Pirated Goods* - https://euipo.europa.eu/ohimportal/en/web/observatory/trends-in-trade-in-counterfeit-and-pirated-goods

[2] Seizures of counterfeit and pirated goods: Top economies of origin of right holders, 2014–16, EUIPO OECD, Trends in Trade in Counterfeit and Pirated Goods, 2019.

[3] The US account for 24.3% of seizures in above-mentioned study, and the EU for 48.6%.

[4] *2020 Status Report on IPR infringement* - https://euipo.europa.eu/ohimportal/en/web/observatory/status-reports-on-ip-infringement

Other studies show the economic harm of piracy on the creative industries. Since the 1980s, digital piracy increased with annually 300 billion visits on illegal websites[5]. In the publishing sector, for instance, the illegal consumption of e-books ranges from 21% of all e-book readers in Germany to 92% of the e-readers in Russia and China[6]. A study quantified the commercial value of music digital piracy in 2015 at USD 29 billion worldwide and estimated that it could grow to USD 53-117 billion in 2022[7]. In Spain, a report commissioned by the creative industries showed that 60% of internet users accessed illegal content up to 11 times a month in 2019, with an estimated lost profit of EUR 2 437 million[8]. Infringing sites constitute a parallel economy that makes hundreds of millions of euros from advertising while maintaining profit margins ranging between 86% and 93%[9].

Most respondents from the creative industries contributing to the public consultation have reported an increase of copyright and related rights[10] infringements online during the COVID-19 pandemic. The lockdown measures taken worldwide have increased users' demand for access to creative content, often from illegal sources. The impact caused by copyright infringements during the pandemic is reported as particularly harmful because a number of other revenue streams for industries, authors and performers, such as theatrical release of films and music concerts, have been interrupted.

In terms of risks to health, consumers and the society, the Qualitative Study[11] on risks posed by counterfeits to consumers, published by the European Observatory on Infringements of Intellectual Property Rights in June 2019, presents an analysis of the RAPEX alerts from 2010 to 2017, which shows that 97% of reported dangerous counterfeit goods were assessed as posing a serious risk to consumers. The most common danger reported (32%) was related to exposure to hazardous chemicals and toxins that could cause acute or long-term health issues from immediate or long-term exposure. 24% of the dangerous products recorded as counterfeit posed more than one danger to users. Toys are the most popular type of product followed by clothing, textiles and fashion items. In fact, the end users of 80% of the goods reported to be dangerous and counterfeit were children (toys, childcare items and children's clothing). As regards the danger to the environment, counterfeit pesticides often contain toxic substances that may contaminate soil, water and food.

---

[5] MUSO report, https://goodereader.com/blog/technology/online-pirate-websites-received-300-billion-visits-globally

[6] See footnote 5.

[7] Frontier Economics Ltd, "The Economic Impact of Counterfeiting and Piracy. A Report Prepared for BASCAP and INTA", p.28-33 (2017): https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAPFrontier-report-2016.pdf

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

[9] The Digital Citizen's Alliance study "Good Money still Going Bad" from 2015.

[10] To facilitate the reading of the document, references to 'copyright' in the Watch List should be understood as references to 'copyright and related rights'.

[11] EUIPO's *Qualitative Study on the risks posed by counterfeiters to consumers* - 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

Since the outbreak of the COVID-19 pandemic, counterfeit and falsified products, such as unproven treatments, test kits and medical equipment and supplies, e.g. masks, ventilators, or gloves, have flooded the European market. To tackle this issue the European Anti-Fraud Office (OLAF) opened an inquiry in March 2020 and has teamed up with nearly all customs and enforcement authorities in Europe and many worldwide, as well as with Europol, Interpol and EUIPO. In the context of this initiative, OLAF has identified more than 800 suspicious companies acting as intermediaries or traders and has contributed to the seizure or detention of more than 14 million counterfeit or substandard items linked to the COVID-19 pandemic.

A report by Europol on Viral Marketing, counterfeits, substandard goods and intellectual property (IP) crime in the COVID-19 pandemic[12] shows that the widespread demand for various products has fueled criminal enterprises to adapt quickly their product portfolios to exploit shortages of genuine products and the fear and anxieties of regular citizens. Some of the counterfeit products distributed risk lives and the safety of frontline workers in healthcare and other essential sectors. A joint study by the EUIPO and the OECD on *Trade in counterfeit pharmaceutical products*[13], which was published on 23 March 2020, shows that in 2016, international trade in counterfeit pharmaceuticals reached EUR 38.9 billion.

The *Internet Organised Crime Threat Assessment*[14] prepared by Europol in 2019 highlights that organised crime groups perform most criminal activity that involves counterfeiting. Such groups employ sophisticated methods for the production and distribution of counterfeit and pirated goods, reaping the benefits of technological advancements. The *Assessment* also underlines that organised crime groups are involved in the production and distribution of counterfeit and falsified medicines. They either have their own infrastructure to manufacture counterfeit medicines in their clandestine laboratories, or import counterfeit medicines from countries outside the EU and repackage and relabel them for distribution within the EU.

The Joint Study by Europol and the EUIPO on IP crime and its link to other serious crime[15] presents case examples showing how intellectual property crime is linked to other forms of criminality, including money laundering, document fraud, cybercrime, food, excise and VAT fraud, bribery and corruption, drug production and trafficking, manslaughter, illegal weapons possession, forced labour and terrorism.

Piracy also has a negative impact 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

[12] Europol's report on *Viral Marketing, counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic* - https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-substandard-goods-and-intellectual-property-crime-in-covid-19-pandemic

[13] OECD-EUIPO Study on *Trade in counterfeit pharmaceutical products* - https://euipo.europa.eu/ohimportal/en/web/observatory/trade-in-counterfeit-pharmaceutical-products

[14] *Internet Organised Crime Threat Assessment* https://www.europol.europa.eu/iocta-report

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

sensitive information or payment card details[16]. 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[17] 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"*[18], the *"Trade for all" Communication*[19], *the IP Action Plan*[20] and the *Strategy for the Enforcement of Intellectual Property Rights in Third Countries*[21] the Commission services have prepared this second edition of the Counterfeit and Piracy Watch List ('the Watch List'). The first edition was published in 2018. The Watch List reflects the results of stakeholder consultations. It lists 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 who 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 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. 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.**

[16] *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

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

[18] COM(2017) 707 final

[19] COM(2015) 497 final

[20] 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

[21] COM(2014) 389 final

The Watch List is a selection of marketplaces and service providers reported by stakeholders. The name of each marketplace and service provider listed is accompanied by a summary of the allegations of the reporting stakeholders and, where provided, a summary of the response of the listed 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 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 Observatory on Infringements of Intellectual Property Rights and the Intellectual Property Crime Coordinated Coalition (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 every opportunity to be heard. In particular, the Commission services invited marketplace operators and service providers listed in the Counterfeit and Piracy Watch List of 2018 to submit written contributions to the public consultation launched in February 2020, so that they could inform the Commission about the actions taken to address the alleged IPR infringements.

Moreover, the Commission services proactively reached out to all the online service providers and marketplace operators that make available their e-mail address in their websites and informed them about the allegations in the contributions to the public consultation pertaining to them. The Commission services invited those service providers and marketplace operators to comment on those allegations. 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 listed 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 listed 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 20 December 2019[22].

2. METHODOLOGY

2.1. Sources

The Commission services conducted a public consultation between 19 February and 1 June 2020[23]. Its results form the basis of the Watch List. 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.

In addition to the support provided by the EUIPO, Europol (Intellectual Property Crime Coordinated Coalition) as well as the EU's Anti-Fraud Office (OLAF), a number of other sources also played a role in the selection process and in defining and describing the listed marketplaces and service providers:

Information from the Commission services

- 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[24];
- Information received from EU Delegations and Offices;

EUIPO reports and studies

- Studies on the economic impact of counterfeiting and piracy[25] and on the trade routes of fake goods[26];
- Sectoral Studies[27];
- Study on Infringing Online Business Models[28];

---

[22] Report on the *protection and enforcement of intellectual property rights in third countries* - https://trade.ec.europa.eu/doclib/docs/2020/january/tradoc_158561.pdf

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

[24] *Report on the EU customs enforcement of intellectual property rights* - https://ec.europa.eu/taxation_customs/sites/taxation/files/2019-ipr-report.pdf

[25] EUIPO-OECD report on *Trade in counterfeit and pirated goods – Mapping the economic impact* - https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Mapping_the_Economic_Impact_study/Mapping_the_Economic_Impact_en.pdf

[26] EUIPO-OECD report on *The real routes of trade in fake goods* - https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Mapping_the_Real_Routes_of_Trade_in_Fake_Goods_en.pdf

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

[28] 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

- Study on Digital Advertising on Suspected Infringing Websites[29];
- Study on Illegal IPTV in the European Union – Research on Online Business Models infringing intellectual property rights[30];
- Qualitative Study on risks posed by counterfeits to consumers[31];
- Joint Study by EUIPO and Europol on IP crime and its link to other serious crime;

Other relevant sources

- Europol status reports[32] and crime threat assessments[33];
- Alexa[34] and SimilarWeb[35] popularity ranks;
- Google Transparency Reports[36];

---

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

[30] *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

[31] EUIPO study on *risks posed by counterfeits to consumers* - https://euipo.europa.eu/ohimportal/fr/web/observatory/news?p_p_id=csnews_WAR_csnewsportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&categoryId=news&journalId=5171912&journalRelatedId=manual/

[32] Europol's *2019 Status report on IPR infringements* - https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Status_Report_on_IPR_infringement/2019_Status_Report_on_IPR_infringement_en.pdf

[33] Europol's report on *Internet organised crime threat assessment* - https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[34] The EUIPO's *Study on Digital Advertising on Suspected Infringing Websites* describes that "Alexa is a web metrics company that provides data about the measure of a website's popularity compared with all of the other websites on the Internet. This data considers both the number of visitors and the number of pages viewed on each visit. Alexa collects traffic data daily from millions of users who have installed the Alexa toolbar and from direct measurements from websites that have incorporated Alexa code, and then uses a proprietary formula to create a popularity ranking for each website. A website's Alexa Rank can be interpreted as the website's position in a league table, with the most popular website given a rank of 1, the next 2 and so on through millions of websites. Alexa provides information about the ranking of websites by country and creates top 500 most popular website lists by country. Alexa also provides a global top 500 ranking representing the most popular websites in the world according to Alexa".

[35] 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".

[36] The EUIPO's *Study on Digital Advertising on Suspected Infringing Websites* describes that "Google regularly receives requests from copyright owners and their agents and organisations that represent them to remove search results that link to content or goods allegedly infringing IP rights. Google makes available online a report that specifies the number of requests it receives to remove search

- Reports by consumer alliances and brand protection companies;
- 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 relevant 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 1 June and 15 October 2020. Consequently, the information included in the report reflects the situation during this period.

All selected marketplaces and service providers are located outside the EU. 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). The contributions of other stakeholders such as e-commerce, social media platforms, providers of internet infrastructure services or associations of providers of technology products and services were also taken into account to select the marketplaces and operators in this Watch List, as they provided information on the measures they take to reduce the availability of counterfeit offers on their platforms. Most of the selected marketplaces and service providers were reported in various contributions, often by stakeholders representing a wide array of sectors.

Some contributions included detailed explanations of the acts performed by the allegedly infringing service providers or service providers' failings as regards duty of care concerning the activities of their users. 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 allegedly infringing 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, Alexa and SimilarWeb web popularity ranks and Google's Transparency Reports for copyright-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

---

results, and indexes the results by domains, copyright holders, reporting organisations and requests. The Google Transparency Report 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 rights holders and other IP content protection associations.

EU right holders and trade with these countries. Searches for popular European content titles or brands were also carried out in order to assess 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*[37] (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 right holders and enforcement authorities) were reported by stakeholders and also taken into account in the preparation of the Watch List.

2.3. Structure

The structure of the Watch List largely follows the structure of the Counterfeit and Piracy Watch List in 2018 ('the 2018 Watch List'). It comprises four main sections:

- online service providers offering or facilitating access to copyright-protected content,

- electronic commerce platforms,

- online pharmacies and service providers facilitating the sales of medicines, and

- physical marketplaces.

One section of this Watch List is dedicated to relevant players in the ecosystem of unauthorised distribution of copyright protected content online. This includes service providers that offer or facilitate, directly or indirectly, access to unauthorised content. It also includes service providers who, reportedly, do not take sufficient action to prevent their users from using their services to offer or facilitate access to unauthorised content. The service providers in this section are grouped in the following categories taking into account their business models and the type of services they provide: cyberlockers, stream-ripping services, linking websites, peer-to-peer and BitTorrent indexing websites, unlicensed download sites, websites for piracy apps, hosting providers, unlicensed IPTV services and social media platforms.

The section on e-commerce platforms reflects the fact that they – differently from the majority of other marketplaces and service providers - facilitate the sales of physical products in an online environment (be it business-to-business, business-to-consumer or consumer-to-consumer sales).

As in the 2018 Watch List, a section is dedicated to online pharmacies. This section identifies illicit online pharmacy networks and the domain name registrars facilitating their operation. These platforms offer for sale all kinds of medicines, including COVID-19-related ones and arrange their delivery to consumers. Due to the major health risks to EU consumers involved, the marketplaces that are reportedly often visited by EU consumers were identified.

---

[37] *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

A final section includes the most prominent physical marketplaces where counterfeit goods are reportedly on sale. Despite the growing significance of online trade, the sales of counterfeit goods in physical marketplaces continue to be rife around the world.

3. RESULTS OF THE PUBLIC CONSULTATION

72 respondents contributed to the public consultation[38]. The majority of the respondents were brand owners, copyright holders, associations and federations representing right holders and associations fighting against IP infringements. Other respondents were individuals, law firms, chambers of commerce and brand protection companies. Some e-commerce, 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 are published along with the Watch List, unless otherwise requested by the respondent.

The reported online and physical marketplaces as well as service providers are from more than 30 countries outside the EU.

Creative industries covering a wide array of sectors, such as music, audiovisual, publishing, TV broadcasting or software, submitted most of the contributions on piracy. The contributions from broadcasters or organisers of broadcast sport events were numerous. They show an increasing concern about the proliferation of operators engaged in the provision of unlicensed IPTV services. This category is included in the Watch List for the first time.

As in 2018, linking websites and cyberlockers were the most frequently reported services. They were followed by unlicensed IPTV operators, peer-to-peer networks and BitTorrent indexing websites and stream-ripping services.

Respondents to the public consultation also showed growing concerns about the significant role of certain actors in addressing proliferation of pirated content, such as social media. This category has been added to the Watch List. Respondents to the public consultation have indicated how some of these service providers, despite their legitimate operations, facilitate online piracy or do not take sufficient measures to avoid or reduce copyright infringements in their services or by their users or clients.

A number of contributions to the public consultation reflect an ongoing debate about the role of Content Delivery Networks[39] (CDNs) in the fight against piracy and the importance of their cooperation with right holders. CDNs might be difficult to categorise, as they usually provide a package of services related to the transmission, delivery and

[38] https://trade.ec.europa.eu/consultations/index.cfm?consul_id=262

[39] 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).

storage[40] of content and relate to various players in the internet ecosystem, including content owners, internet access providers, domain name owners, hosting service providers and cloud service providers. CDNs could be described as a layer in the internet infrastructure: the services provided by CDNs contribute to the correct functioning of the internet, as they improve the efficiency and security of the transmission of information. At the same time, the fact that the IP addresses of CDNs' clients are not publicly accessible makes enforcement of IPR more difficult.

US-based *Cloudflare*, not listed in this Watch List, has been reported in this context by some stakeholders calling on the service to improve its cooperation with right holders including its responsiveness to infringement notices, and its practices when opening accounts for websites to prevent illegal sites from using its services. *Cloudflare* has reported that making generally available certain sensitive information about host IP addresses would jeopardise the protection of their clients' websites from threats or cyberattacks. *Cloudflare* has also reported that it takes appropriate steps, through robust abuse reporting system and a Trusted Reporter programme, to ensure that right holders have the necessary information to pursue complaints of alleged infringements with the hosting providers and website operators able to act on those complaints. Court decisions in Germany[41], Italy[42] and the United States[43] have provided some guidance on how CDNs should react to right holders' requests. However, the debate continues. Increased cooperation between CDNs and right holders should contribute to facilitating the enforcement of the rights infringed by CDNs' clients.

Brand owners (electronics, fashion, footwear, luxury, pesticides, sporting goods, toys), brand associations and federations, chambers of commerce, brand protection companies, associations fighting against counterfeiting and law firms reported mostly physical marketplaces and e-commerce platforms. More than 60 e-commerce platforms from more than 20 countries were reported for the online distribution of allegedly counterfeit goods. E-commerce platforms remain the marketplaces that brand owners indicate primarily for inclusion in the Watch List for the high volume of counterfeit goods sold online. Some of these platforms are active at regional level; others have a global reach.

Respondents to the public consultation also showed growing concerns about the role of certain social media platforms in the distribution of counterfeit goods online. A report[44] by the Transnational Alliance to Combat Illicit Trade (TRACIT) showed that "*fraudulent advertising is rapidly emerging as a new risk to consumers shopping online, where millions of consumers are exposed to thousands of fraudulent advertisements taking them*

[40] Depending on the business model and systems architecture used by individual CDNs, storage may be temporary, i.e. to store the information to ensure its smooth transmission, or permanent, e.g. in case cloud infrastructure is part of the services provided.

[41] Judgement in preliminary injunction proceedings: Cologne District Court, case 14 O 171/19, 30 January and 9 October 2020.

[42] Order issued by the Court of Rome XVII (formerly IX) Civil Section, on 24 June 2019 - R.G.26942/2019.

[43] New York federal court – Case 1:17-cv-00726-LMB-JFA (October 2016) - *Cloudflare* was ordered to identify the operators of Libgen and Bookfi in the context of wider proceedings brought against the two sites and Sci-Hub.

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

to thousands of illegitimate e-commerce websites that defraud and/or sell counterfeit products and deceitful services".

Some e-commerce and social media platforms as well as other service providers provided detailed information on the measures they take to reduce the availability of counterfeit offers 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[45], which is a voluntary agreement facilitated by the European Commission to prevent offers of counterfeit goods from appearing in online marketplaces.

The European pharmaceutical industry provided an update on illicit online pharmacy networks and domain name registrars that facilitate the online sales of counterfeit medicines. The reported domain name registrars allegedly continue not having or not enforcing policies against counterfeit medicines. The European pharmaceutical industry reported more than 600 websites for selling counterfeit or falsified medicines.

The National Association of Boards of Pharmacy (NABP) has identified a high number of new domain names that were registered for illicit purposes in March 2020 that contained terms such as 'covid', 'corona' and 'virus'. The vast majority of these websites allegedly belongs to seven illicit online pharmacy networks assisted by a handful of domain name registrars. A few e-commerce platforms were also reported for the online sales of counterfeit medicines. The European pharmaceutical industry did not nominate social media platforms.

Concerning physical marketplaces, most of the responses were submitted by brand owners from the following sectors: automotive spare parts, cosmetics, electronics, fashion, food and beverages, footwear, jewellery, luxury, pesticides, sport and toys. Chambers of commerce, associations fighting against counterfeiting, law firms and also a few associations from the creative sectors nominated physical marketplaces. Physical marketplaces from more than 30 countries were reported, the majority of which are located in China and South and Southeast Asia. The number of physical marketplaces reported by stakeholders in Africa has increased. Many of those listed in the 2018 Watch List continue to be reported. The majority of the physical marketplaces continue to function also either as a distribution hub or wholesale market for counterfeit goods. Free trade zones in the United Arab Emirates continue to be a concern for stakeholders in many sectors in terms of the import of counterfeit goods into the European Union.

4. POSITIVE DEVELOPMENTS SINCE THE 2018 WATCH LIST

Since the 2018 Watch List, several enforcement actions and measures have been taken by enforcement authorities, right holders and the owners, operators and landlords of marketplaces and service providers. Consequently, some of the marketplaces or service providers listed in the 2018 Watch List are no longer mentioned in this Watch List. Others may be not mentioned, despite continued concern expressed by right holders, for reasons such as their diminished popularity or relevance as an example for the purposes of this Watch List. The European Commission welcomes these actions and measures and

[45] *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

encourages enforcement authorities, right holders and the owners, operators and landlords to continue combating piracy and counterfeiting.

Lazada, a Thai platform, made efforts over the past two years to reduce the volume of counterfeit offers on its platform. Lazada introduced a more stringent IPR policy, started educating its sellers, improved its responsiveness regarding IPR concerns and strengthened cooperation with right holders and enforcement authorities. Lazada also actively participated in the drafting of the Memorandum of Understanding facilitated by the Thai authorities between online sales platforms and brand owners, and reportedly stands ready to join the scheme once concluded.

NAVER, the Korean platform, has also stepped up efforts against counterfeiting over the past two years. NAVER joined the Memorandum of Understanding between sales platforms and brand owners signed with the aim to reduce the volume of counterfeit offers on e-commerce platforms in Korea and facilitated by the Korean authorities, which shows an effort to improve cooperation with stakeholders and the enforcement authorities. In April 2020, NAVER also signed Cooperation Agreements for Verification with 45 brand owners to improve the platform's responsiveness.

A joint task force consisting of KIPO, the Seoul Special Judicial Police, the Korean Intellectual Property Agency and some brand owners carried out focused enforcement actions in the shopping district **Dongdaemun** for two weeks in August 2019. As a result, the enforcement authorities seized 170 counterfeit goods, with a corresponding value of about EUR 100 000 euro and 22 people were found implicated in criminal activity.

KIPO established an online team of 110 people for the monitoring of counterfeit goods on e-commerce platforms. In 2019, the online monitoring team suspended 129 128 online offers of counterfeit goods. In 2019, a total of 376 people received criminal charges of trademark infringement, and 6 269 797 counterfeit goods were seized.

Due to the enforcement actions by Dubai Police and the Dubai Department of Economic Development (DED) the volume of counterfeit goods has started to decrease in **Dragon Mart**.

In 2019, the enforcement authorities of the United Arab Emirates has seized a considerable value of counterfeit goods in **Ajman Free Trade Zone**, mainly in the following product categories: shoes, bags, clothes, perfumes, accessories, headsets and printer inks.

Openload, which used to be one of the most popular streaming cyberlockers worldwide that offered unauthorised copies of films, books and music, shut down in October 2019[46].

Torrentz2 was a BitTorrent indexing website that allegedly emerged in 2017 following the closure of *Torrentz.eu*. It provided access to a range of content, including allegedly unauthorised copies of films, TV programmes, software, videogames and music. It was shut down by Belgian Customs and the Public Prosecutor's Office of Brussels on 29 June 2020.

Mp3va, which was a popular website engaged in the unlicensed sale of music content, was removed from this year's Watch List, because it lost popularity over the past two

[46] https://descrier.co.uk/technology/openload-and-streamango-shut-down-in-deal-with-anti-piracy-group/

years after United States credit and payment providers at the request of right holders voluntarily decided to stop providing services to this website.

1channel.ch, which was one of the most visited linking or referrer sites globally at the time of publication of the 2018 Watch List, is reportedly offline now.

Rnbxclusive.review, which was a popular linking site in 2018, is reportedly offline now. A domain name using the word "rnbxclusive" has been active since May 2020, but the link with the site listed in the 2018 Watch List is not confirmed.

5. NEXT STEPS

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. The Commission services engage in IP Dialogues and IP Working Groups with partner countries around the world, including those with which an agreement covering IP issues is in force. In this context, since the 2018 Watch List, the Commission has had such dialogues or working groups with countries of the Andean Community (Colombia, Peru and Ecuador), Central America, Canada, China, Hong Kong (China), South Korea, Taiwan, Thailand, Turkey, Ukraine and the United States.

The Commission services will continue using the Watch List also in the framework of the EU technical cooperation activities, including IP Key China[47], Southeast Asia[48] and Latin America programmes[49].

The Commission services will update the Watch List regularly, including by taking into account any comments that the marketplaces and service providers included in this Watch List may submit about the allegations referred to below. They will also continue monitoring the measures and actions taken by the local authorities in relation to the listed marketplaces and service providers as well as the measures and actions taken by the service providers and marketplace owners to curb IPR infringements.

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

Online marketplaces 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 right holders. These service providers rely on other online service providers such as reverse proxy services, caching services, hosting providers or 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 right holders to prevent or restrict unauthorised acts. Several respondents to the public consultation emphasised the increasing importance of streaming piracy, including of films and live sports events, as opposed to piracy offering the download of content.

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

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

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

Several contributions pointed to the main factors that lead to the reported copyright infringements, namely inadequate criminal enforcement against online copyright infringements in certain jurisdictions or inadequate legal frameworks for incentivising cooperation by relevant players. Some of the listed 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. This section lists service providers that offer content protected by copyright and service providers that directly or indirectly facilitate access to this content. The listed 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 2018 Watch List. This Watch List includes two new sub-sections to take account of growing concerns regarding the role of various services in copyright infringements online: unlicensed IPTV service providers and social media.

6.1. 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 right holder.

Stakeholders report that the cyberlockers listed in this section generally 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 6.3 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.

Stakeholders report that more than half of all cyberlockers are responsible for malware infections on users' computers. Moreover, users may be subject to identity theft and viruses when using them.

Cyberlockers are reported to obtain 70.6% of their revenue from the sale of premium accounts[50], which offer users different kinds of benefits (such as increased download speeds). These premium accounts are popular among those users who download large,

[50] *Behind the Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions*. https://fia-actors.com/fileadmin/user_upload/News/Documents/2014/Oct/dca-netnames-cyber-profibility-ph11.pdf

mainly audiovisual, files. 29.4% of the cyberlockers' revenues come from online advertising.

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.

Uptobox - uptobox.com

Stakeholders across different sectors, including software and audiovisual, have reported *Uptobox* for inclusion in this Watch List.

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 owner is allegedly located in Switzerland, with links to the United Arab Emirates. 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. Some stakeholders report that it usually takes *Uptobox* over 140 days to remove infringing content reported by right holders.

Uptobox has a global SimilarWeb ranking of 1 985. Its ranking in France is 246. It had 27.6 million visits in June 2020, 37.42% of them from France.

Rapidgator - rapidgator.net

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

Rapidgator is a direct download cyberlocker, hosted in Switzerland but allegedly operated from Russia. Russian courts issued a blocking injunction against *Rapidgator* in 2019[51]. However, the site is still accessible from other countries. Legal action concerning *Rapidgator* also includes decisions issued in Germany[52].

Rapidgator allegedly offers access to infringing music, films, TV programmes, books and video games. It generates revenues through online advertising. It also sells premium ad-free subscriptions with additional benefits such as unlimited download speed, unlimited simultaneous downloads, instant downloads without any wait restriction and download of large files. It provides incentives for users to upload popular content such as films, music and books. These incentives include monetary rewards as well as affiliate schemes[53].

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

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

[53] By using an affiliate scheme, other websites (the affiliates) have a link to the cyberlocker website. If a user clicks on that link and downloads content, the cyberlocker pays a commission to the affiliate.

Rapidgator reportedly generates approximately USD 3.7 million in annual revenue[54]. Stakeholders report that *Rapidgator* offers right holders 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.

Rapidgator has a global SimilarWeb ranking of 1 578. It had 29 million visits in June 2020, 28.26% of them from Japan.

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

Stakeholders across different sectors, including publishing, music, audiovisual and broadcasting, 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. It is reportedly among the top 4 favourite services for e-book piracy[55]. Legal action concerning this operator includes blocking orders issued in Germany[56], India[57] and Italy[58]. The Bundesgerichtshof (Germany) submitted a reference for a preliminary ruling on the activities of *Uploaded* to the Court of Justice of the European Union in 2018[59].

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 high numbers of downloads of their uploaded content. Registration options for users include free or premium accounts. Premium account holders have access to full speed ad-free downloads, unlimited storage for uploaded files, unlimited simultaneous downloads and earning options.

Uploaded.net has a global SimilarWeb ranking of 2 362. It had 25.88 million visits in June 2020, 38.36% of them from Japan.

4shared – 4shared.com

Stakeholders across different sectors, including publishing and music, continue reporting *4shared* for inclusion in this Watch List.

---

[54] See footnote 50.

[55] https://www.statista.com/statistics/688411/book-piracy-sites/

[56] District Court of Munich I, 21 O 6197/14, 10 August 2016: https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2016-N-14540?hl=true&AspxAutoDetectCookieSupport=1

[57] 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

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

[59] Elsevier Inc. v Cyando AG (Case C-683/18), judgment pending: http://curia.europa.eu/juris/document/document.jsf?text&docid=211268&pageIndex=0&doclang=en&mode=lst&dir&occ=first&part=1&cid=2395393

4shared is a popular direct download cyberlocker. It reportedly offers unauthorised copies of music, e-books (over one million titles), films and TV shows. It features its own search index and a player to stream the audio files it stores. It is reportedly registered in the British Virgin Islands and its owner is probably located in the United States[60]. Legal action concerning this operator includes a blocking order issued by the Korean Communications Standard Commission in 2014[61].

4shared gets income from advertising and from its basic and premium accounts. It allegedly offers a reward scheme for users who upload popular content. Its mobile apps that enable users to stream content to mobile devices reportedly give access to infringing content as well.

In response to the allegations made by other stakeholders, *4shared* has reported that the main purpose of their service is to offer private storage, and only a small portion of the files stored is subject to takedown notifications. Their terms of use provide that upload of copyright-protected content is not authorised. Its Copyright Policy complies, according to *4shared*, with relevant US law for the purposes of removing unauthorised content. *4shared* has also informed that they offered right holders the possibility to have moderation accounts that enable them to remove swiftly allegedly unauthorised content. Other tools that *4shared* claims to use to prevent unauthorised content include music content recognition technologies and code filters to block files that are identical to those previously reported.

4shared has a global SimilarWeb ranking of 2 993. It had 9.41 million visits in June 2020, 30.98% of them from Brazil.

Wi.to and Ddl.to

The music industry has reported wi.to and ddl.to for inclusion in this Watch List as cyberlockers.

An operator established outside the EU allegedly manages both wi.to and ddl.to. Although their popularity in terms of global ranking is lower than that of other sites included in this Watch List, the music industry reports both cyberlockers as particularly harmful due to the alleged presence of pre-released content in their services.

Ddl.to automatically redirects users to ddownload.com, which offers premium account options to its users.

Wi.to has a global SimilarWeb ranking of 54 508. It had 837 520 visits in June 2020, 45.13% of them from the United States. Ddl.to has a global SimilarWeb ranking of 47 565. It had 918 150 visits in June 2020, 15.59% of them from Japan.

Dbree - dbree.org

The music industry has reported Dbree for inclusion in this Watch List as a cyberlocker.

This cyberlocker allegedly makes available copyright-protected content online without

[60] https://myip.ms/info/whois/204.155.146.95/k/2053208960/website/4shared.com

[61] 19th standing committee of the Korean Communication Standards Commission (KCSC), decision of 14 October 2014: http://transparency.kr/case/258

authorisation from right holders. Stakeholders report that it has been recently launched but is capitalising on the popularity of another unconnected cyberlocker, dbr.ee, which shut down in 2019. It obtains revenue from advertising.

Although its popularity in terms of global ranking is lower than that of other sites included in this Watch List, the music industry reports it as particularly harmful due to the alleged presence of pre-released content in its services.

Dbree has a global SimilarWeb ranking of 40 350. It had 953 120 visits in June 2020, 27.49% of them from the United States.

6.2. 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 platforms[62]. 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, usually in mp3 or mp4 format, with certain metadata, such as the title of the content or name of the author, added to it. According to the relevant right holders, 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 music and film industries, stream-ripping is currently the most prominent form of piracy globally.

Y2mate and YouTubeconverter - y2mate.com and youtubeconverter.io

Stakeholders from the music industry have reported Y2mate and YouTubeconverter for inclusion in this Watch List as stream-ripping services.

Y2mate and YouTubeconverter are interconnected stream-ripping services allegedly managed by one single operator. YouTubeconverter automatically redirects its users to Y2mate to obtain the corresponding mp3 or mp4 file.

Y2mate reportedly offers various ways to download music content or music videos from video sites, including YouTube. This includes a search function that helps the user locate the desired content and select the format of the downloaded content.

[62] 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.

Legal action concerning Y2mate includes blocking orders in Italy[63] and Spain[64]. Legal action concerning YouTubeconverter includes blocking by internet service providers in Spain[65].

Y2mate has a global SimilarWeb ranking of 278. It had 114.87 million visits in June 2020, 8.52% of them from Brazil. YouTubeconverter has a global SimilarWeb ranking of 24 595. It had 1.44 million visits in June 2020, 6.93% of them from Brazil.

Savefrom - Savefrom.net

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

Savefrom is a stream-ripping service allegedly operated outside the EU.

Savefrom offers the user the possibility to download mp3 files, after downloading the site's Video Downloader software. This software downloads an audio-only mp4 from YouTube to the user's device; the user's device then converts it into an mp3 file.

Savefrom has a global SimilarWeb ranking of 289. It had 131.88 million visits in June 2020, 11.01% of them from India.

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

Stakeholders from the music industry have reported Flvto and 2conv for inclusion in this Watch List as a stream-ripping service.

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 includes judgments or blocking orders in Australia[66], Denmark[67], Italy[68] and Spain[69].

Flvto has a global SimilarWeb ranking of 584. It had 54.3 million visits in July 2020, 16.74% of them from Brazil. *2conv* has a global SimilarWeb ranking of 1 430. It had 25.57 million visits in July 2020, 18.73% of them from Germany.

6.3. Linking or referring websites

Linking or referring websites aggregate, categorise, organise and index links to content

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

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

[65] See footnote 64.

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

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

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

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

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, do 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.

The music and film industries are particularly concerned, since, allegedly, linking sites often make available pre-release content. The music and film industries have reported that the listed service providers received notices to take down content or cease and desist letters, but they have reportedly not reacted and have not removed the content upon request.

Fullhdfilmizlesene - Fullhdfilmizlesene.com* or *.org[70]

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

Fullhdfilmizlesene is a Turkish-language website that reportedly facilitates access to unauthorised copies of films by aggregating, categorising (by genre, new movies, most recommended and most viewed), organising and indexing links to video hosting services and cyberlockers. It features a search bar and its operator regularly updates it with new releases. It is hosted in Turkey and uses domain privacy and proxy services to hide the identity and residence of the operator.

Fullhdfilmizlesene has a global SimilarWeb ranking of 3 131. It had 9.60 million visits in June 2020, 88.68% of them from Turkey.

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 claims to have 16 054 accessible files, organised in alphabetical order. It also features a search bar. The website is allegedly hosted in Russia and the residence of the operator is assumed to be outside the EU. Legal action concerning this site includes blocking orders in Russia[71] and Spain[72].

Seasonvar offers free access or a premium subscription that allows users to download or

[70] Fullhdfilmizlesene.org redirected to Fullhdfilmizlesene.com at the time of publication of this Watch List.

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

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

stream HD audiovisual content without any advertising interruptions.

Seasonvar has a global SimilarWeb ranking of 1 408. It had 45.82 million visits in June 2020, 33.4% of them from Ukraine.

Swatchseries - Swatchseries.to

Stakeholders from the audiovisual industry continue reporting *Swatchseries* (*Dwatchseries.to* in the 2018 Watch List) for inclusion in this Watch List.

Swatchseries reportedly facilitates access to television content that is streamed without the authorisation of the right holders. It is hosted in Switzerland and uses services to mask its IP location. This site has been subject to blocking orders in Belgium[73], Denmark[74], Italy[75], Norway[76] and Singapore[77].

This site has a global SimilarWeb ranking of 2 034. It had 27.04 million visits in June 2020, 40.68% of them from the United States.

Rlsbb - Rlsbb.ru

Stakeholders from the music, audiovisual and software industries have reported *Rlsbb* as a website offering links to copyright-infringing content, including music, films, videogames and e-books.

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, including some of those included in this Watch List. The website is organised as a blog divided into categories to enable users to find the articles related to the titles they are searching for. Even if some links are removed, the website invites users to add new links to the same content in the comments sections. It uses services to mask its IP location. It is allegedly hosted in the United States. Legal action concerning this website includes blocking orders in Belgium[78], Denmark[79], Italy[80] and Portugal[81].

The website allegedly obtains revenues from advertisements in pop-up banners.

Rlsbb has a global SimilarWeb ranking of 8 137. It had 5.86 million visits in June 2020, 35.09% of them from the United States.

---

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

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

[75] AGCOM Order Proc. N. 1168/DDA/LC - http://swatchseries.to

[76] Oslo District Court, case 16-072899TVI-OTIR/08, 22 June 2016.

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

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

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

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

[81] 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.

Rezka.ag

Stakeholders from the audiovisual industry have reported *Rezka* as a website streaming copyright infringing content.

Rezka is a popular Russian-language streaming website hosted in Russia.

It allegedly offers illegal streaming of 22 500 movies, 5 500 TV series, as well as cartoons and anime. Users can search and filter content by genre, year and categories. Legal action concerning this website includes blocking injunctions or orders in Belgium[82], Russia[83] and Spain[84].

Rezka has a global SimilarWeb ranking of 1 412. It had 46.13 million visits in June 2020, 53.27% of them from Ukraine.

6.4. 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[85]. 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. Once users have downloaded the BitTorrent client, they need to locate the content they want to download and click on the torrent file or the magnet link associated to the file in question. By doing this, the BitTorrent client starts receiving pieces of the file from the seeders. Once the BitTorrent client has received all the pieces of the file, it reassembles them into the completed file and saves the file on the computer of the person who initiated the download.

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.

The Pirate Bay - ThePirateBay.org

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

---

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

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

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

[85] 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

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. 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[86], Australia[87], Austria[88], Belgium[89], Denmark[90], Finland[91], France[92], Greece[93], Iceland[94], India[95], Ireland[96], Italy[97], Netherlands[98], Norway[99], Portugal[100], Romania[101], Russia[102], Singapore[103], Spain[104], Sweden[105] and the United Kingdom[106]. The Court of Justice of the European Union has

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

[87] 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

[88] 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

[89] 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

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

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

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

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

[94] 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

[95] 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

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

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

[98] 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

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

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

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

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

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

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

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

also confirmed that *The Pirate Bay* infringes copyright[107]. However, the service reportedly continues operating through multiple alternative domains hosted in various countries around the world.

The Pirate Bay has a global SimilarWeb ranking of 1 434. It had 26.65 million visits in June 2020, 21.34% of them from the United States.

Rarbg - Rarbg.to

Stakeholders from the music industry continue reporting *Rarbg* for inclusion in this 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. The content is organised and displayed in categories. *Rarbg.to* is one of the BitTorrent indexing websites responding to take down notices, but right holders report that the same infringing material is usually quickly reposted on the site. Legal action concerning this website and its variants includes judgments or blocking orders in Australia[108], Denmark[109], Finland[110], Greece[111], India[112], Indonesia, Ireland[113], Italy[114], Singapore[115] and the United Kingdom[116].

Rarbg reportedly generates income from advertisements and a pay-per-install distribution model for potential malware[117].

Rarbg has a global SimilarWeb ranking of 659. It had 41.87 million visits in June 2020, 26.6% of them from the United States.

---

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

[107] 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

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

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

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

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

[112] 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

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

[114] 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

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

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

[117] 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

Rutracker - Rutracker.org

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

Rutracker is a BitTorrent website that was reportedly launched in 2010 following the shutdown of *Torrent.ru* in Russia. It has around 1.5 million active torrents and 13.9 million registered users. The site is hosted in Russia by a Seychelles company. Legal action concerning this site includes blocking orders in Russia[118] and Singapore[119].

Rutracker has a global SimilarWeb ranking of 875. It had 40.05 million visits in June 2020, 45.92% of them from Russia.

1337x - 1337x.to

Stakeholders from the music and audiovisual industries continue reporting *1337x* and its proxies for inclusion in this Watch List.

1337x is a BitTorrent website that allegedly allows users to download films, TV programmes, music, games and apps. Users can sort the content by genre, year and language. Moreover, the music section is divided into the sections such as 'Popular Today', 'Popular This Week', 'Trending Today', 'Trending This Week', and 'Top 100 This Month'. The identification of its actual host is not possible, as the site is masked behind a reverse proxy service. Legal action concerning this website includes judgment or blocking orders in Australia[120], Austria[121], Belgium[122], Denmark[123], Greece[124], India[125], Ireland[126], Italy[127], Singapore[128] and Spain[129].

---

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

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

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

[121] 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

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

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

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

[125] 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

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

[127] 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

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

The website obtains revenues from advertisements and Bitcoin donations.

1337x has a global SimilarWeb ranking of 548. It had 53.61 million visits in June 2020, 15.31% of them from the United States.

6.5. Unlicensed download sites

Unlicensed download sites engage in the unlicensed distribution of content. The sites under this category 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 have reported *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. Any type of user can use the site to browse content; however, in order to purchase and download music, the user is required to register and create an account. 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.

The site claims to have over 1.5 million tracks available offering a wide range of international music repertoire, which it updates daily. One-minute demos of the songs on the site are available without logging in to a user account. The Russian language version of the site notes that registered users can request albums. The site also offers an affiliate programme to engage partners that earn a percentage of all the payments made by the customers they attract.

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

Legal action concerning this site includes blocking by internet service providers in

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

Greece[130] and Denmark[131].

Music Bazaar has a global SimilarWeb ranking of 215 422. It had 117 170 visits in June 2020, 23.48% of them from the United States.

***Sci-hub* (*Sci-hub.tw*; *sci-hub.cc; sci-hub.ac; sci-hub.bz; sci-hub.ren; sci-hub-im; sci-hub.shop*)**

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.

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." 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[132], which ruled that the site was liable for wilful infringement of copyrights.

Sci-hub allegedly gains unauthorised access to publishers' journal databases by using compromised user credentials obtained via phishing frauds[133]. 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.

Sci-hub.tw has a global SimilarWeb ranking of 1 777. It had 25.34 million visits in June 2020, 27.16% of them from China.

Library Genesis - Libgen.is and mirror sites

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

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

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

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

[132] 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/

[133] 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).

by the Italian Regulatory Authority for Communications[134] and by courts in France[135], Greece[136], Russia[137] and the United Kingdom[138], it has shut down and reopened with different names and mirror sites over the years.

Libgen.is is, at the time of publishing this Watch List, one of the most popular websites in the Library Genesis Group. It is hosted in both Russia and the Netherlands and operated from Russia. It allegedly operates a repository of pirated publications, including books, scientific, technical and medical journal articles as well as scholarly materials. It has a number of mirror sites making the same content available, such as *libgen.lc*, *libgen.io*, *libgen.pw* and *gen.lib.rus.ec.* They reportedly obtain the vast majority of the scientific, technical and medical journal articles via *Sci-hub* (see above).

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

Libgen.is has a global SimilarWeb ranking of 4 392. It had 7.79 million visits in June 2020, 16.54% of them from the United States.

Bookfi.net (mirror sites *booksee.org*, *bookre.org*, or *bookzz.org*) is another important website of the Library Genesis Project. It is reportedly operated from Russia or Ukraine. It allegedly makes available more than 2.2 million unauthorised copies of books. The site was subject to blocking orders in Denmark[139] and the UK[140]. Advertising is a source of income for the site, which also invites users to make donations. *Bookfi.net* has a global SimilarWeb ranking of 33 842. It had 1.23 million visits in June 2020, 16.54% of them from Russia.

B-ok.org is another relevant website in the Library Genesis Project included in the 2018 Watch List that was subject to a blocking order in Denmark[141] and reportedly continues to operate as *z-lib.org* and mirror sites such as *1lib.eu*, *b-ok.cc*, *booksc.org*, *book4you.org*, *bok.org*, *bookos-z1.org* and *booksc.xyz*. The site is allegedly operated from China. It allegedly offers illegal access via free download to more than 5.1 million books (it claims to be "the world's largest e-book library") and more than 77 million articles. Users who register with email and password are able to increase their daily downloads limit, use an e-book converter, submit book reviews and use other features. It obtains revenues from donations, payments of "gift cards" and fund-raising activities. *z-lib.org* has a global SimilarWeb ranking of 26 645. It had 2.84 million visits in June

---

[134] 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

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

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

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

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

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

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

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

2020, 14.76% of them from the United States.

6.6. Websites for Piracy Apps

Certain websites make available apps that provide their users with access to pirated films and TV programmes. Piracy Apps attract millions of consumers who often pay for subscriptions.

Popcorn Time

Stakeholders from the audiovisual industry continue reporting *Popcorn Time* for inclusion in this Watch List.

Popcorn Time is allegedly a Piracy App with high global audience numbers and available in various forms and languages. The website's operator is reportedly located in North Africa. Once installed, the users of the application have access to more than one thousand films and TV programmes, allegedly made available without authorisation of the copyright holders. Legal action concerning this app includes blocking injunctions in Belgium[142], Denmark[143], Italy[144], Norway[145] and the United Kingdom[146].

The website where users can find the app's file, *popcorntime.app*, has a global SimilarWeb ranking of 41 902. It had 1.22 million visits in June 2020, 14.49% of them from Brazil.

6.7. Hosting providers

Pirate sites often depend on hosting providers that provide the necessary infrastructure for them to operate (for instance easy access or fast download). Thus, hosting providers are in a good position to stop or prevent infringements.

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.

Private Layer

Stakeholders from the audiovisual industry continue reporting *Private Layer* for

[142] District Court Mechelen, 2015/076, 20 October 2015.

[143] District Court of Frederiksberg, order: 969/2017; link: https://rettighedsalliancen.dk/wp-content/uploads/2020/02/Frederiksberg-District-Court-RA-v-TDC-5-December-2017-Popcorn-Time-EN.pdf

[144] News item: https://www.repubblica.it/tecnologia/sicurezza/2015/08/31/news/l_italia_sequestra_popcorntime_il_netflix_pirata-121956859/

[145] The Norwegian Economic Crime Unit (ØKOKRIM), 13 September 2017: https://www.okokrim.no/inndrar-bruksretten-til-popcorn-time-no.6028617-411472.html

[146] High Court of Justice; Chancery Division [2015] EWHC 1082 (Ch), Case No. HC2014 –002029, 28 April 2015.

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 right holders.

6.8. Unlicensed IPTV services

Unlicensed IPTV services offer without authorisation access via streaming to hundreds or even thousands of TV channels illegally sourced from legitimate service providers worldwide[147]. 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 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. Some unlicensed IPTV services sell their apps in "unofficial" app stores or websites[148], 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 them how to use those apps to stream the infringing content that the unlicensed IPTV services provide[149]. 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

[147] See footnote 30.

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

[149] 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.

precise location of an IPTV operator.

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.

King365tv.com

King365tv.com reportedly operates from Algeria. It allegedly gives access to over 2 200 international channels and an extensive VoD library. The site attracts around 75 000 monthly visitors to purchase a subscription. More than 70% of the traffic reportedly comes from France.

VolkaIPTV.com

VolkaIPTV.com reportedly operates from Algeria or Morocco. It 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. More than 67% of the traffic reportedly comes from France.

Electrotv-sat.com

Electrotv-sat.com reportedly operates from Morocco. It offers reseller options, card sharing and customer plans of various IPTV services that provide access to over 16 000 international TV channels and large VoD libraries at low monthly subscription fees. It has an estimated audience of over 40 000 users.

6.9. Social media

This category includes providers of extremely popular services that stakeholders from various sectors have reported for inclusion in this Watch List. Stakeholders generally acknowledge that the services mentioned in this Section do 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, a number of stakeholders who have contributed to the public consultation have raised concerns about the growing number of uses of these services to infringe copyright.

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.

Stakeholders claim that the service providers referred to in this Section take limited action to solve or prevent infringements of copyright taking place in their services. The service providers are not reported as having engaged in unauthorised activities, but are mentioned in this Section for the reason that they are reported to allegedly lag behind in efforts to combat piracy or counterfeiting.

VK.com (V Kontakte)

Stakeholders from the publishing and audiovisual industries have reported *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, with more than 500 million accounts. Right holders report that *VK.com* users can have unauthorised access to films and TV shows, including via embedded video players, as well as books, including textbooks. 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.

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 right holders to report infringements. However, *VK.com* is included 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 response to the allegations made by other stakeholders, *VK.com* has reported that its current policies have given rise to 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 informs that they have in place a special procedure for removal of unlicensed content that right holders may report by filling out an online form. *VK.com* reports that they have handled more than 1.36 million claims, the vast majority of which end up in content removal, with a response time of less than 24 hours. Moreover, *VK.com* informs that they have put in place content identification technologies to prevent the availability of unauthorised content in their service. Finally, *VK.com* reports that a lot of content available in the service has been uploaded by the right holders or is subject to licences concluded between *VK.com* and other service providers, including Russian television networks and streaming providers.

VK.com has a global SimilarWeb ranking of 14. It had 1.75 billion visits in June 2020, 78.79% of them from Russia, where it is the second most visited website.

Telegram

Stakeholders from the publishing, music and broadcasting industries have reported *Telegram* for inclusion in this Watch List.

Telegram is a cloud-based mobile and desktop application. It reportedly has its legal domicile in the United Kingdom and its operational centre in the United Arab Emirates.

Telegram offers instant messaging services. It is mentioned in this Section because stakeholders report that Telegram users use other means to communicate with each other, including public "channels", which have similar features as social media, to share unauthorised content for download or streaming, including music, books, news publications, films and television programmes, to promote unlicensed IPTV services. Subscribers also share links to other sites hosting copyright-protected content or to other marketplaces selling counterfeit goods and pharmaceutical products.

Telegram is included in this Watch List because stakeholders report insufficient responsive action from Telegram when they report infringements.

Telegram reportedly has 400 million monthly users and is the most downloaded social media application in over 20 countries. The mobile application has been downloaded over 100 million times from the Google Play Store.

In response to the allegations made by other stakeholders, Telegram claims that they do not tolerate any malicious content on their platform and delete within 24 hours when reported by the Autorità per le Garanzie nelle Comunicazioni AGCOM or by stakeholders by e-mail. For instance, Telegram shut down the 26 channels in Italy following an order issued by AGCOM[150]. Some stakeholders have indeed reported that Telegram is more responsive since then. Telegram has also indicated that their efforts in fighting malicious content on their platform have been very successful in other areas, including terrorist propaganda and child abuse.

7. E-COMMERCE PLATFORMS

In the midst of COVID-19 pandemic, more and more consumers turn to e-commerce platforms due to lockdowns or in order to reduce risk of contracting COVID-19. 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. The joint OECD-EUIPO study on the misuse of small parcels for trade in counterfeit goods[151] shows that a vast majority of the products that were seized during the period examined (63% of the total number of customs seizures of counterfeit and pirated goods worldwide) concerned small parcels.

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 the *Recommendation on measures to effectively tackle illegal content online*[152] published on 1 March 2018. The Recommendation outlined certain principles and safeguards that, in the interest of the internal market and the effectiveness of tackling illegal content online and in order to safeguard the balanced approach of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

[150] https://www.agcom.it/documents/10179/18569712/Comunicato+stampa+29-05-2020+1590755948700/e145aaaa-60b7-488e-a313-e54f08088173?version=1.0

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

[152] 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

(E-commerce Directive)[153], should guide the activities of the Member States and of the service providers in identifying, preventing reappearance of and removing illegal content.

The Recommendation identifies best practices, which online platforms are encouraged to follow in order to reduce the availability of illegal content, including counterfeit offers on e-commerce websites. The Recommendation aims 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, right holders and enforcement authorities.

In the course of the public consultation stakeholders, while acknowledging that e-commerce platforms do not infringe IPR or base their business models on activities that infringe IPR, reported that certain 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 right holders 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 the non-use of effective automated risk management tools to identify high-risk behaviours and potential red flags were considered.

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, Amazon and eBay (*Aliexpress.com*, *Tmall.com*, *Taobao.com*, *1688.com*[154], *Amazon.com*[155] and *eBay.com*[156]). Out of the three the most frequently reported e-commerce platforms are those of Alibaba, followed by Amazon and eBay. Stakeholders reported also this year that, despite their efforts, a significant volume of counterfeit goods allegedly remain available on these platforms damaging, among others, the creative, electronics, crops, fashion, musical instruments, sport, food, luxury, cosmetics and toys industries. At the same time, these platforms' level of compliance with the *Recommendation on measures to effectively tackle illegal content online*[157] remains higher than that of the below listed e-commerce platforms. They have improved their enforcement tools to prevent and filter counterfeit offers. The operators of these platforms are generally open to cooperate with right holders, including as signatories of the *Memorandum of Understanding on the sale of counterfeit goods via the internet*[158]. *eBay*, *Amazon* and *Alibaba* also contribute to the work carried out by the EUIPO to develop tools and mechanisms that facilitate the protection of IPR. *Amazon*

[153] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML

[154] Platforms operated by *Alibaba*

[155] Platform operated by *Amazon*

[156] Platform operated by *eBay*

[157] See footnote 37.

[158] See footnote 45.

and *Alibaba* attend awareness-raising and other meetings organised by Europol. *Amazon* also created an online IPR investigation team ('Counterfeit Crime Unit') to enhance the cooperation with right holders, 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 on this Watch List. It is noted, however, that according to stakeholders further progress is needed to ensure that offers of counterfeit goods disappear from these platforms or are significantly reduced.

Notably, stakeholders urge these platforms to carry out more thorough identity checks of the vendors, and to sanction them for hiding their real identity by removing their accounts. Stakeholders call also for further improvement of automated tools by these platforms, in particular to be able to link the data of new vendors to accounts that were previously suspended or restricted, thus eliminating the risk of repeat infringers returning to the platform. Such improvement, stakeholders raise, should also include checking active accounts to prevent multiple (unjustified) accounts. Stakeholders call on these platforms to introduce caps on a number of identical goods that can be offered by non-business sellers and set out more elaborate identity checks for individual sellers offering high volume of goods. Stakeholders encourage these platforms to simplify their brand protection programmes to make them more user-friendly. Stakeholders also suggest providing additional guidance to sellers, which would urge them to upload more and better photos of the actual goods offered. Such guidance should reject unauthorised use of catalogue pictures, use of pictures that do not show, or hide or blur the labels and brands of the goods in order to provide more data points for the automatic filtering/monitoring tools.

Bukalapak

Stakeholders from the engineering and technology, fashion, luxury, sports, tobacco, alcohol, entertainment, health and beauty sectors continue reporting *Bukalapak* for inclusion in this Watch List. *Bukalapak* is one of the most popular, mostly business-to-consumers, online e-commerce platforms in Indonesia, allegedly selling a high volume of counterfeit goods in the following product categories: electronics, clothing, fashion accessories, books, films, mobile phones, car and motor spare parts and industrial goods. Allegedly, the majority of the goods on this platform originates from mainland China. Stakeholders report a new negative development on the platform, which is that *Bukalapak* started to offer for sale allegedly counterfeit pesticides.

Stakeholders have reported *Bukalapak* mainly because of the unreasonably long processing time to remove infringing offers, for the overly burdensome web form used by the platform for requesting takedowns, for the low number of proactive measures applied to detect and remove counterfeit offers and for not applying any prohibition for the use of contentious keywords in the listings, such as "replica".

In response to the allegations made by other stakeholders, *Bukalapak* has reported that its Terms and Conditions strictly prohibit the sales of IPR-infringing goods on its platform. *Bukalapak* has in place a notice and takedown procedure to remove IPR-infringing offers from its platform and applies proactive measures to filter and block such offers. *Bukalapak* has reported that it cooperated also with enforcement authorities, regulators and other administrative bodies as well as brand owners. *Bukalapak* has participated in awareness-raising and other events related to IPR, including those organised by the IP Key Southeast Asia Programme.

Dhgate

Stakeholders from the food, fashion, luxury, pesticides, jewellery, musical instruments and sport industries 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 in the following product categories: food and beverages, fashion accessories, jewellery, clothing, footwear, leather goods, sport equipment and watches. Stakeholders report the platform also for the alleged sales of counterfeit pesticides.

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, but these have not led to the significant decrease of counterfeits on this platform.

In response to the allegations made by other stakeholders, *Dhgate* has reported that in order to reduce health risks, it does not permit the sales of food and beverages as well as pesticides. *Dhgate* has informed that it has in place a notice and takedown system to remove illegal listing, that it regularly removes infringing offers flagged by stakeholders and that it has closed many sellers' accounts due to IP infringements.

Dhgate has reported cooperation with certain brand owners and an IP protection organisation and has shown openness to discuss with right holders how to improve the user-friendliness of its notice and takedown procedure. *Dhgate* has acknowledged that there is room for improvement in its proactive measures and has indicated that new actions are planned for the future. *Dhgate* has informed that it is planning to step up efforts to improve the vetting of sellers.

Tiu.ru, ***Prom.ua***, ***Bigl.ua***, ***Deal.by*** and ***Satu.kz***

Stakeholders from the engineering and technology, fashion, luxury, sports, toy, tobacco, alcohol, entertainment, health and beauty sectors continue reporting several marketplaces owned by *EVO Company Group* for inclusion in the Watch List. The following marketplaces were reported: *Tiu.ru* (Russia), *Prom.ua* (Ukraine), *Bigl.ua* (Ukraine), *Deal.by* (Belarus) and *Satu.kz* (Kazakhstan). The most important ones respectively, in Russia and Ukraine, are *Tiu.ru* and *Prom.ua*. *Tiu.ru* and *Prom.ua* are among the largest business-to-consumers marketplaces in Russia and Ukraine, allegedly selling a high volume of counterfeit goods in the following product categories: car and motor spare parts, clothing, footwear and accessories, engineering and electronics, materials for repair, beauty and health, sport, leisure goods and books.

The marketplaces were nominated mainly because of the takedown procedure, which includes overly burdensome administrative requirements, the overly long processing time to handle complaints, the lack of responsiveness by the legal team to notifications of infringing listings as well as because of the inconsistency in taking action upon notifications of IPR infringements and for rejecting protection of international trademarks registered at WIPO and designated to the host country of the marketplace.

Mercado Libre

Stakeholders from the electronics, food, fashion, luxury, musical instruments, pharmaceuticals and creative and cultural industries reported *Mercado Libre* for inclusion in the Watch List. *Mercado Libre* is one of the most popular business-to-consumers e-commerce platforms in Brazil and in Latin America, selling a high volume of allegedly counterfeit goods in the following product categories: food and beverages, clothing, footwear, electronics and leather goods. Stakeholders also reported that *Mercado Libre* allegedly offers for sale counterfeit COVID-19 response products (e.g. gloves, masks, test kits and medicines).

Stakeholders have reported this marketplace mainly because of the allegedly inconsistent enforcement requirements, unreasonably long response times to notifications of IP infringements and for the low number of proactive measures applied by the platform.

Stakeholders acknowledge that certain improvements have been implemented over the past years, including the better cooperation with right holders, but these have not led to the significant decrease of counterfeits on this platform.

In response to the allegations made by other stakeholders, *Mercado Libre* has underlined that it maintains a strong commitment to fight against counterfeit and pirated goods on its platforms. Led by this objective, *Mercado Libre* informed that it had launched an improved notice and takedown procedure in December 2019. According to *Mercado Libre*, the new tool 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 machine learning technologies). *Mercado Libre* has indicated that it cooperates with certain right holders and associations as well as with enforcement authorities. *Mercado Libre* claims to be in compliance with the majority of the best practices in the Commission *Recommendation on measures to effectively tackle illegal content online*[159].

Shopee

Stakeholders from the electronics, fashion, food, luxury, pesticides, pharmaceutical and sport sectors reported *Shopee* for inclusion in the Watch List. *Shopee* is one of the biggest business-to-consumers online e-commerce platforms in Southeast Asia, with its headquarters in Singapore. It allegedly sells a high volume of counterfeit goods in Southeast Asia in the following product categories: watches, jewellery, leather goods, clothing, fashion accessories, food and beverages as well as sport equipment. Stakeholders report the platform also for the alleged sales of counterfeit pesticides and pharmaceuticals.

Stakeholders claim that the branches in Malaysia, Taiwan, Thailand, Indonesia and Vietnam are allegedly the most problematic, because they offer more counterfeit goods relative to other national platforms. The branches in Singapore and the Philippines allegedly cause serious difficulties for the brand owners to enforce their rights.

Stakeholders have reported these marketplaces operated by *Shopee* mainly because of the lack of responsiveness to notifications of infringing listings, for the inconsistent and

[159] See footnote 37.

burdensome requirements in relation to information required to support enforcement and for the failure to apply repeat infringer policy. Stakeholders also report that no proactive measures are applied to detect or remove what they consider obviously counterfeit offers. The processing time is up to two weeks for removing infringing offers, which stakeholders deem unreasonably long.

In response to the allegations made by other stakeholders, *Shopee* has reported that it has a policy that strictly prohibits the sales of counterfeit goods on its platforms. It also has in place notice and takedown procedures that enable brand owners to notify counterfeit offers on its platforms. *Shopee* has reported that it handles complaints within one week if it receives a valid complaint with complete documentation. *Shopee* has informed that it applies proactive measures to filter infringing offers, cooperates with stakeholders and enforcement authorities and has taken part in awareness-raising activities related to IPR enforcement.

Snapdeal

An association with members from various sectors, including the engineering and technology, fashion, luxury, sports, tobacco, alcohol, entertainment, health and beauty sectors continue reporting *Snapdeal* for inclusion in the Watch List. *Snapdeal* is one of the most popular business-to-consumers online e-commerce platforms in India It allegedly sells a high volume of counterfeit goods in the following product categories: jewellery, leather goods, clothing, fashion accessories, food and beverages as well as sport equipment.

Stakeholders have reported this marketplace mainly because of the insufficient implementation of the platform's policies against IP infringements, for the insufficient detection and removal of illegal listings and for the ineffective vetting of sellers.

In response to the allegations made by other stakeholders, *Snapdeal* has reported that it has a policy and guidelines that strictly prohibit the sales of counterfeit goods on the platform. It also has a policy to vet sellers. *Snapdeal* has reported that it applies proactive and preventive measures to filter counterfeit offers, has in place a notice and takedown procedure that enables brand owners to notify counterfeit offers on the platform, and it applies severe sanctions in the case of an infringement. *Snapdeal* has also introduced a brand protection program that provides additional protection and privileges for brands with registered trademark. *Snapdeal* has informed that it uses machine-learning technologies to detect repeat infringers. *Snapdeal* has reported that it cooperates also with enforcement authorities and brand owners.

Tokopedia

Stakeholders from the book publishers, cosmetics, electronics, fashion, food, luxury, sport and toy sectors reported *Tokopedia* 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 in the following product categories: academic textbooks, clothes, sport goods (footwear, football jerseys), electronics, food and beverages, jewellery, leather goods, watches, cosmetics and toys.

Stakeholders have reported this marketplace mainly because of the ineffectiveness of the proactive measures to detect and filter counterfeit offers, for the failure to apply a repeat infringer policy and for the burdensome requirements to notify IPR infringements.

Reportedly, there is no prohibition of the use of contentious keywords in the listings, such as 'replica'. Some sellers of counterfeit goods have allegedly been active on *Tokopedia* for seven years, which raises doubts about the effectiveness of the platform's enforcement efforts.

In response to the allegations made by other stakeholders, *Tokopedia* has reported 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.

Xxjcy.com and China-telecommunications.com

A stakeholder specialised in brand protection that monitors e-commerce platforms with a data-driven technology covering various sectors (e.g. luxury, fashion, technology, pharmaceuticals and healthcare) continues reporting *Xxjcy.com* and *China-telecommunications* for inclusion in the Watch List. *Xxjcy.com* and *China-Telecom* are popular business-to-business marketplaces in China, selling a high volume of allegedly counterfeit goods in the following product categories: construction machinery, chemical machinery, clothing, engine parts, fashion accessories, textile products, lights and lighting products and furniture. *China Telecommunications* and *Xxjcy* are assumed to be linked, because they have exactly the same adverts and layouts when searching keywords across the platform The business strategy of the platforms does not allow the users to purchase through the sites; instead, they are given the option to contact the seller to make purchases outside the platforms.

This platform has been reported mainly because of the alleged inefficiency of its policy to vet sellers, to use proactive measures to detect illegal listings, for the failure to respond to the notifications of IPR infringements as well as for the failure to efficiently apply and enforce sanctions against repeat infringers.

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

The joint study of the EUIPO and the OECD on *Trade in counterfeit pharmaceutical products*[160], which was published on 23 March 2020, shows that in 2016, international trade in counterfeit pharmaceuticals reached EUR 38.9 billion. Counterfeit medicines not only cause economic loss for the pharmaceutical industry, but also constitute a serious threat to public health.

The study finds that counterfeit antibiotics, sexual impuissance pills or lifestyle medicines, as well as painkillers were the most often counterfeited. Customs officials also frequently seized other medicines, like counterfeit cancer, malaria or HIV treatment drugs, diabetes treatment medicines, local anaesthetics as well as epilepsy, blood pressure or heart disease medication. Counterfeit pharmaceuticals may contain too little, too much or none of the active ingredient contained in the genuine medicine. They may also have been manufactured under unsanitary conditions or may contain contaminants.

[160] EUIPO-OECD Study on *Trade in counterfeit pharmaceutical products* - 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

The revenue loss for EU governments linked to tax evasion by counterfeiters of medicines amounts to EUR 1.7 billion. The vast majority, 96% of all customs seizures of counterfeit medicines, are postal or express courier deliveries[161]. The social cost of counterfeit medicines is also high. The job losses are estimated at more than 80 000 jobs per year in the EU pharmaceutical sector and other related sectors.

According to the study, the majority of counterfeit medicines originate from China, Hong Kong (China), Singapore and India. China and India are the main producers of counterfeit medicines, whereas the United Arab Emirates, Singapore and Hong Kong (China) serve as transit hubs. African countries, Europe and the United States appear to be the main destinations of fake medicines.

The COVID-19 pandemic has also shown that criminals quickly adapt to the new trade environment and find their way to infiltrate the legitimate supply chain of pharmaceuticals. Counterfeit and falsified products, such as unproven treatments, test kits and medical equipment and supplies – masks, ventilators, gloves, etc. – have flooded the European market. A recent report from the National Association of Boards of Pharmacy (NABP)[162] has identified many illicit online pharmacies claiming to sell prescription drugs marketed for COVID-19 treatment. NABP found that over 90% of the COVID-19-related domain names identified were registered anonymously, which makes it difficult for enforcement authorities to investigate these sources. These illegal sites advertise and sell falsified and counterfeit medicines and vaccines claiming to prevent and treat COVID-19. A high number of new domain names were registered for illicit purposes in March 2020 that contained terms such as 'covid,' 'corona', and 'virus'.

A joint industry initiative led by the Pharmaceutical Security Institute[163] (PSI), which started in April 2020 with the monitoring of 27 medicines likely linked to the COVID-19 pandemic and offered by online pharmacies, showed similar trends as those identified by PSI in the previous three years concerning other medicines sold online. Out of the more than 350 traditional websites identified as selling COVID-19 related medicines, more than 84% are from the same illicit online pharmacy networks, using the same domain name registrars that have already been actively engaged in the sales of fake medicines in the past three years.

The Communication from the Commission on the EU Security Union Strategy[164] also draws attention to illicit online pharmacy networks in the section on organised crime.

It is reported that certain domain name registrars knowingly sponsor illicit online pharmacy networks. Pursuant to the Registrar Accreditation Agreement concluded

[161] According to the 2016 Study published by Legiscript[161], globally only 4% of internet pharmacies operate lawfully. The estimate is that around 30 000-35 000 illicit online pharmacies are active on the internet and fail to adhere to applicable legal requirements, sell prescription medicines without requiring a valid prescription or sell counterfeit, falsified or substandard medicines.

[162] National Association of Boards of Pharmacy's *Rogue RX activity report* - https://nabp.pharmacy/wp-content/uploads/2020/05/Rogue-Rx-Activity-Report-May-2020-1.pdf

[163] The Pharmaceutical Security Institute is a non-profit membership organisation dedicated to protecting public health, sharing information on counterfeiting of pharmaceuticals and initiating enforcement action through the appropriate authorities.

[164] Communication from the Commission on *an EU Security Union Strategy* - https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf

between ICANN[165] and the registrars, registrars are obliged to take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse by their clients, including to the sales of counterfeit or falsified medicines.

These registrars do not allegedly comply with the Registrar Accreditation Agreement, ignore abuse notifications submitted by right holders on the sales of fake medicines and do not suspend the domain names of illicit online pharmacies.

Consequently, according to the European pharmaceutical industry, the online distribution of medicines has increased over the past two years and this is only partly caused by COVID-19. Another joint industry initiative led by PSI showed that online service providers, including domain name registrars and registries, have cooperated less with the pharmaceutical industry over the last two years. Domain name registrars and registries rarely suspend the domain names of allegedly illicit pharmacies, when the pharmaceutical companies notify them of IP infringements. According to the European pharmaceutical industry, fewer and fewer domain name registrars enforce policy against counterfeit medicines and historically prudent domain name registrars have become less reactive to notifications.

PSI reported far better responsiveness by social media platforms than by domain name registrars and registries. Reportedly, 88% of illicit offers (888 out of 1 014) were removed from social media platforms in recent projects conducted by PSI (D-18 and D-19[166]). The compliance rate of social media platforms reported by the European pharmaceutical industry varies between 4 and 87%.

A number of challenges arise concerning the use of domain names by illicit online pharmacies. The use of domain privacy and proxy services that act as intermediaries for domain registrations is a standard practice for illicit online pharmacies. The contact details of the proxy service appear in the WHOIS Database instead of the contact details of the actual registrant. Such services are often located in jurisdictions where it is difficult to require and obtain information on their users.

Another emerging practice for the online sales of counterfeit medicines is the use of subdomains to conceal infringing content. It often happens that the domain itself (e.g. domain.com) does not have any content and appears to be offline, but counterfeit or falsified medicines are sold on websites appearing on a subdomain (e.g. subdomain.domain.com). These subdomains are advertised and communicated directly to the consumers through various channels, including messaging services, emails and social media platforms.

According to the European pharmaceutical industry, the typical rogue network models continue including customer service call centres, back-end merchant accounts with acquiring banks and a medicine distribution system. The operators of illicit online pharmacies usually own clusters of hundreds of websites, some of which are the anchor

[165] The Internet Corporation for Assigned Names and Numbers is an American multi-stakeholder group and non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet.

[166] The Pharmaceutical Security Institute conducts an operation every year to disrupt the online distribution channels of falsified and counterfeit medicines.

websites where the actual sales take place[167]. Most of them are websites that funnel internet users back to the anchor websites, while the rest are sleeping websites used only when an active website is shut down by the enforcement authorities. The websites are promoted through search engine optimisation and email spams.

This Watch List focuses in this section on the same domain name registrars as listed in the 2018 Watch List. These domain name registrars, according to the European pharmaceutical industry, continue being non-responsive to abuse notifications and are often used by rogue online pharmacy networks that offer to deliver medicines also to EU Member States.

CJSC Registrar R01 (registrar) **serving *EVA Pharmacy, PharmCash online pharmacy networks***

CJSC Registrar R01 is a domain name registrar that reportedly continues to serve many rogue internet pharmacies. It continues to provide domain name registration services to *EVA Pharmacy* and *PharmCash*, which are reportedly illicit online pharmacy networks offering for sale counterfeit medicines as well as prescription medicines without requiring the prescription. The business model of these networks has not changed over the past two years. These networks use many referral[168] websites. Almost all of the active websites affiliated with these networks redirect users to a less visible online pharmacy website. The use of referral internet pharmacies allows the continuous operation of the network, because their redirection patterns can be changed easily anytime, including when a destination anchor online pharmacy has been suspended or disabled.

The following registrars were reported for serving these and other illicit online pharmacy networks and for not cooperating with right holders in disrupting illicit online pharmacy networks: *Registrar of Domain Names Reg.Ru, Regtime Ltd* and *R01-RU* from Russia, *GKG.Net* from the United States, *Paknic Private Limited* from Pakistan and *Afriregistar* from Burundi.

EPIK Inc. *(registrar)* **serving *RxProfits* online pharmacy network**

EPIK Inc. is a domain name registrar that, according to the European pharmaceutical industry, provides domain name registration services to, among others, illicit online pharmacies, such as *RxProfits* network. *RxProfits* is an internet pharmacy network that allegedly offers counterfeit medicines as well as prescription medicines to consumers without requiring a prescription. This network always uses referral websites. Almost all the active websites (99%) affiliated with *RxProfits* redirect users to a less visible internet (anchor) pharmacy website, the *pharmacy-xl.com*. This anchor website processes transactions for approximately 500 networked referral internet pharmacies. In addition to offering worldwide shipping, the network actively advertises some controlled substances, including *Xanax*, *Valium*, *Soma*, *Ambien*, and *Tramadol*.

In response to the allegations made by other stakeholders, *EPIK Inc.* has reported that it complies with the applicable laws and if the court orders it, *EPIK Inc.* terminates the

[167] According to the 2016 Study published by Legiscript, globally only 4% of internet pharmacies operate lawfully. The estimate is that around 30 000-35 000 illicit online pharmacies are active on the internet and fail to adhere to applicable legal requirements, sell prescription medicines without requiring a valid prescription or sell counterfeit, falsified or substandard medicines.

[168] Referral is a recommendation from one website to another.

provision of domain name registration services to the relevant pharmacy networks. *EPIK Inc.* has reported that it is not in a position to adjudicate whether or not any of the registrants notified by complainants are engaged in an illegal activity. Therefore, it refers the complainants to the court system, which can adjudicate in these matters. *EPIK Inc.* has emphasised also that it complies with the Registrar Accreditation Agreement concluded with ICANN.

ZhuHai NaiSiNiKe Information Technology Co. *(registrar)* **serving *PharmaWeb* online pharmacy network**

ZhuHai NaiSiNiKe Information Technology is a domain name registrar that, according to the European pharmaceutical industry, allegedly provides domain name registration services to illicit online pharmacies, such as *PharmaWeb* network. *PharmaWeb* is an internet pharmacy network that reportedly offers counterfeit medicines and has connections with Canada. The network mostly targets the US market, but the medicines sold are distributed from countries outside the US, including Italy, South Africa, New Zealand, India, the United Kingdom, Israel, Switzerland, Fiji and Canada. Although the network markets itself as a Canadian pharmacy, consumers using a Canadian IP address cannot access these websites. Blocking access from the country in which the operation is based is a common tactic used by illegal pharmacies networks.

9. PHYSICAL MARKETPLACES

Despite the growing popularity of e-commerce platforms, the majority of counterfeit goods, in terms of volume, continue being sold in physical marketplaces. Stakeholders reported physical marketplaces from all five continents, which shows that physical marketplaces that offer counterfeit goods to consumers or to retailers continue being widespread around the world. Physical marketplaces continue selling both high and low quality counterfeit goods[169]. Many of the physical marketplaces reported by stakeholders are located in areas frequented by tourists and in free trade zones.

The OECD Council adopted a *Recommendation on Countering Illicit Trade: Enhancing Transparency in Free Trade Zones* on 21 October 2019. The main purpose of the recommendation is to enhance transparency in free trade zones in order to prevent criminal organisations from taking advantage of them.

Argentina

La Salada, Buenos Aires

Stakeholders continue reporting *La Salada* for inclusion in the Watch List. *La Salada* is located in Buenos Aires and allegedly remains one of the biggest wholesale and retail marketplaces of counterfeits in Latin America. It is located in an area of more than 20 hectares where over 15 000 stands sell all kinds of products, most of them allegedly counterfeit. *La Salada* is divided into three sub-marketplaces: *Ocean*, *Hurkupiña* and *Punta Mogotes*, each one of which has its own administrators and rules. This marketplace

[169] As described in the EUIPO study *Mapping the economic impact of trade in counterfeit and pirated goods*: "*In primary markets, prices are expected to be close to those of legitimate products, whereas larger price dispersions are expected in secondary markets. Consumers that knowingly purchase an IP infringing product may expect to pay a lower price for it than for a genuine product".*

allegedly offers for sale a high volume of counterfeit goods, including clothing, footwear, toys, perfumes, cell phones, accessories and other consumer electronics.

Despite the raids and arrest of the suspect leaders of the market, along with some associates in the last two years, stakeholders report that illegal activities and counterfeiting continue flourishing on the market and further actions and continued efforts are needed to cleanse this marketplace from counterfeiting.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Argentina, for instance on *La Salada de Mendoza* and on *Santa Rosa de Lima* in Buenos Aires.

Brazil

Rua 25 de Março, São Paulo

Stakeholders report the *Rua 25 de Março* Market for inclusion in the Watch List. *Rua 25 de Março* is located in São Paulo. It is, with its surrounding areas, including *Galeria Pagé*, *Shopping 25 de Março* and the neighborhoods of *Bras* and *Santa Ifigenia*, allegedly the biggest wholesale and retail marketplaces of counterfeits in Brazil. These marketplaces allegedly offer for sale a high volume of counterfeit goods, including clothing, footwear, toys, perfumes, cell phones, accessories and other consumer electronics.

In 2019, a successful enforcement operation with the participation of an international enforcement team was conducted, in the framework of which 10 tons of counterfeit goods, mainly cosmetics and toys were seized, with an estimated value of EUR 2.3 million. The operation, called "*Promitheia*" showed a successful cooperation between DIREP[170] and São Paolo's local authorities. Despite this and other successful operations, the market remains one of the biggest in Brazil, allegedly offering high volume of fakes.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Brazil, for instance on *Mercado Popular de Uruguaiana* and *Feirão des Malhas* in Rio de Janeiro, *City of Nova Serrana* in Nova Serrana, on *Feire de importados* in Brasilia as well as on *Juta Gallery* and *Galeria Tupan* in São Paulo.

Canada

Pacific Mall, Markham

Stakeholders continue reporting the *Pacific Mall* for inclusion in the Watch List. The *Pacific Mall* is located in Markham, Ontario and remains one of the biggest retail shopping malls in Canada. It covers around 25 000 square metres and has around 500 retail shops allegedly selling mainly counterfeit goods of Chinese origin. The *Pacific Mall* allegedly continues offering for sale a high volume of counterfeit clothes, footwear, toys, car spare parts, cameras, cell phones, computers and other electrical appliances, cosmetics, perfumes, health and beauty products, houseware, jewellery, watches and optical products.

[170] Divisão de Repressão ao Contrabando e Descaminho

Despite the efforts of the market owner, the scale of counterfeiting on this marketplace reportedly continues being high. Both the operators and the local authorities are urged by the stakeholders to take further actions in order to reduce the availability of counterfeit goods.

Other marketplaces in Canada, such as *Dixie, Weston, Dr. Fleas Flea Markets* and *Downsview Park Merchants Market* in Toronto, *Saint Eustache Flea Market* in Quebec as well as *747 Flea Market* in Brampton in Ontario were also reported by stakeholders for the sale of high volume of counterfeit goods.

China

***Huaqiangbei Electronics Markets, Shenzhen* (*Yuan Wang Market, Manhar Digital Plaza, Longsheng Market* and *Mingtong Market*)**

Stakeholders continue reporting the *Huaqiangbei Electronics Markets* for inclusion in the Watch List. *The Huaqiangbei Electronics Markets*, which include *Yuan Wang Market, Manhar Digital Plaza, Longsheng* Market and *Mingtong Market,* are located in Shenzhen and are among the biggest wholesale and retail marketplaces in China. There are dozens of multi-storey shopping complexes filled with distributor shops in Huaqiangbei District in Shenzhen that allegedly continue being a central hub for counterfeit consumer electronics.

Despite the raids, the *Huaqiangbei* tech malls reportedly continue conducting counterfeit sales allegedly due to non-cooperation on the part of the mall management and shop owners. As a result, counterfeiting reportedly persists with little actual deterrence. Stakeholders have reported the following *Huaqiangbei* tech malls as particularly problematic: *Yuan Wang Market*, *Manhar Digital Plaza*, *Longsheng Market* and *Mingtong Market*.

Asia Pacific Xingyang Fashion and Gifts Plaza and Asia Pacific Shenghui Leisure and Shopping Plaza, Shanghai

Stakeholders continue reporting the *Asia Pacific Xingyang Fashion and Gifts Plaza* and *the Asia Pacific Shenghui Leisure and Shopping Plaza* for inclusion in the Watch List. These plazas are located in Shanghai, in Pudong District, and are among the biggest retail plazas in China. These plaza marketplaces allegedly continue offering for sale a high volume of counterfeit clothes and accessories, cosmetics as well as footwear. The two markets are interlinked and operated by the same landlord.

Right holders report that almost all the goods continue being counterfeit and authorities rarely perform any raids in these markets. Despite the landlord's efforts to remove counterfeits, high volumes of counterfeits are available on these marketplaces. Right holders have investigated and have taken enforcement actions over the last two years against some sellers in these plazas, but they report that these efforts have not led to the reduction of the sale of counterfeit goods.

Anfu Market and its neighbourhood, Putian City

Stakeholders continue reporting the *Anfu Market* for inclusion in the Watch List. *Anfu Market* is located in Putian City, Fujian Province and allegedly remains one of the biggest wholesale marketplaces for counterfeit shoes in China. Besides, *Anfu* Market allegedly sells also counterfeit luxury goods and clothing. The goods sold on *Anfu*

Market are reportedly manufactured and stored before distribution in *Licheng District* (mostly in *Huangshi town*, *Qibu village*, *West Tianwei town*), *Chengxiang District* (mainly *Huating Industrial Park*) and *Xiuyu District*. *Anfu* Market is open only during the night. The merchants of *Anfu* Market continue engaging in online sales, including the sales of expensive counterfeits. Many counterfeit shoes sold on Chinese and other sales platforms are allegedly from *Anfu* Market.

Stakeholders report that it continues being difficult to take action against counterfeiters in *Anfu* Market and its neighbourhood. The local authorities reportedly remain unresponsive to right holders' complaints and the number of raids has not increased either over the past two years to reduce the availability of counterfeits. Stakeholders report that, to mitigate the risk of raids, factories usually ship all the products to a nearby warehouse after the production is complete or the manufacturers split the production process into different steps and each step is finished in different workshops.

Mule Town in Guangxi Province

Stakeholders continue reporting *Mule Town* for inclusion in the Watch List. *Mule Town* is located in the eastern part of Guiping City and it allegedly remains one of the biggest wholesale and retail marketplaces for counterfeit leisure sport goods. The main products sold in *Mule Town* are jerseys of popular football teams and World Cup national jerseys.

Many counterfeit garment factories are reportedly located on the east side of the town, mainly concentrated in the industry zones (around 35 factories are allegedly in the area). The practices of the rogue merchants on this market have not changed over the past two years. Reportedly, only a small number of large factories keep 10 000-20 000 sets of counterfeit sportswear in stock, the rest manufacture the finished products in neighbouring workshops while the fabric-cutting and processing are done inside the factories. At night, the finished products are transported to warehouses in rural areas for storage. Warehouses are usually located in Zhenlong Town or Gaotang Village.

Stakeholders report that it continues being difficult to take actions against counterfeiters in *Mule Town*. The local authorities reportedly remain unresponsive to right holders' complaints and the number of raids to reduce the availability of counterfeits has not increased over the past two years either.

Silk Market, Beijing

Stakeholders report the *Silk Market* for inclusion in the Watch List. The *Silk Market* is located in Beijing, and it is allegedly one of the biggest retail marketplaces for counterfeit goods in China. The marketplace is also a tourist attraction. The *Silk Market* allegedly offers for sale a high volume of counterfeit goods, including clothing, footwear, handbags and wallets.

Over the past two years, stakeholders reportedly initiated civil litigations against the landlords and the sellers. Despite several administrative and criminal raids, the market operator does not cooperate to reduce the availability of counterfeits on the market. Stakeholders report that it is difficult to take actions against counterfeiters and counterfeits have reportedly become more visible in the past two years.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in China, for instance on *Dajingkou Shoes and Clothing Market* in

Qingyang Town, *Shenyang Wu Ai Market*, *Guangzhou Baiyun World Leather Trading Center* and *Luohu Commercial City*.

Colombia

San Andresitos, Bogota

Stakeholders report *San Andresitos* for inclusion in the Watch List. The *San Andresitos* markets are located in Bogota and are allegedly one of the biggest shopping areas in Colombia for counterfeit goods. There are three main *San Andresitos* in Bogota, two of them in the city center (*San Andresito San Jose* and *San Andresito de la 38*), one in the Northern part of the city (*San Andresito del Norte*). *San Andresitos* allegedly offer for sale a high volume of counterfeit goods, including watches, footwear, electronics, accessories, bags, cell phones and medicines.

Stakeholders report that it is difficult to take actions against counterfeiters in *San Andresitos*. The local authorities reportedly remain unresponsive to right holders' complaints and the number of raids on these marketplaces is low.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Colombia, for instance in *Mall San Andresitos* in Medellin, on *Open Markets* and *Palacio National* in Bogota.

India

Karol Bagh Market, Tank Road Market and Gaffar Market, Delhi

Stakeholders continue reporting *Karol Bagh Market, Tank Road Market and Gaffar Market* for inclusion in the Watch List. *Karol Bagh Market, Tank Road Market and Gaffar Market* are located in Delhi and they are among the biggest marketplaces in India for allegedly counterfeit goods. These marketplaces allegedly offer for sale a high volume of counterfeit goods, including sports goods, footwear, clothing, electronics, luxury goods, watches and cosmetics.

According to stakeholders, some civil and criminal enforcement actions have been taken over the last two years resulting in successful seizures of counterfeits, which however has not proved to be effective enough.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in India, for instance on *Lajpat Rai Market, Arya Samaj Road* and *Hardiyan Singh Road* markets as well as *Sarojini Nagar* market in Delhi, the *Crawford Market* in Mumbai, *Khidderpore* Market in Kolkata or the *Sector 18, Atta Market* in Noida as well as *Heera Panna* and *Manish Market* in Mumbai, *AC Market* in Ludhiana, *Greater Kailash M Block, Palika Bazaar* in New Delhi, *Sadar Patrappa Market, Brigade Road* and *Commercial Street* markets in Bengaluru.

Indonesia

Mangga Dua Market, Jakarta

Stakeholders continue reporting *Mangga Dua Market* for inclusion in the Watch List. The *Mangga Dua Market* is located in Jakarta and it is allegedly one of the biggest wholesale and retail marketplaces in Indonesia for counterfeit goods. This marketplace

allegedly offers for sale a high volume of counterfeit goods, including handbags, fashion accessories and clothing.

The local authorities reportedly remain unresponsive to right holders' complaints and the number of raids has not increased either over the past two years to reduce the availability of counterfeits.

Tanah Abang, Jakarta

Stakeholders report *Tanah Abang Market* for inclusion in the Watch List. The *Tanah Abang Market* is located in Jakarta and it is allegedly one of the biggest wholesale and retail marketplaces for counterfeit goods in Indonesia and in Southeast Asia. The marketplace allegedly offers for sale a high volume of counterfeit goods, including textile products, clothing and electronics.

Only very minimal raid actions appear to be possible due to the lack of authority of the Governor's Office over IP crime. The local authorities reportedly remain unresponsive to right holders' complaints and the number of raids is low.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Indonesia, for instance on *ITC Cempaka Mas*, *ITC Kuningan* and *Ambassador Market, Pasar Cipulir, Pasar Jatinegara, Pasar Senen, Pusat Grosier Cililitan* in Jakarta, *Tangerang* in Banten and *Kute Seminyak* in Bali.

Malaysia

Petaling Street Market, Kuala Lumpur

Stakeholders continue reporting *Petaling Street Market* for inclusion in the Watch List. The *Petaling Street Market* is located in Kuala Lumpur and it is allegedly one of the biggest wholesale and retail marketplaces for counterfeit goods in Malaysia. This marketplace is also a tourist attraction. The marketplace allegedly offers for sale a high volume of counterfeit goods, including clothing, footwear, handbags and perfumes.

The local authorities reportedly remain unresponsive to right holders' complaints and only very minimal raid actions appear to be possible due to alleged lack of manpower in the enforcement authorities.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Malaysia, for instance on *Taman Johor Jaya* market in Johor Bharu, the *Berjaya Time Square* market, *the Jalan TAR* open market, the *Low Yat Plaza* and the *Tamaran Johor* market in Kuala Lumpur as well as the *Batu Ferringhi* Night Market in Penang.

Mexico

El Tepito, Mexico City

Stakeholders continue reporting *El Tepito* for inclusion in the Watch List. *El Tepito* is located in Colonia Morelos in the Cuauhtémoc borough of Mexico City and it is allegedly one of the biggest wholesale and retail marketplaces for counterfeit goods in Mexico. This marketplace allegedly offers for sale a high volume of counterfeit goods,

including electronics, fashion, luxury, sport goods, watches and toys. Allegedly, most of the counterfeit goods come from China, being stored in tunnels and secret warehouses.

Stakeholders report that *El Tepito* market remains dangerous, making it almost impossible for right holders to enforce their rights and posing challenges for enforcement authorities. Despite the success of some raids, in most cases the merchants allegedly revert soon to sale of counterfeits.

San Juan de Dios Market, Guadalajara

Stakeholders report *San Juan de Dios Market* for inclusion in the Watch List. *San Juan de Dios Market* is located in the Mexican State of Jalisco, in Guadalajara, and it is allegedly the biggest wholesale and retail indoor marketplace for counterfeit goods in Mexico and one of the biggest in Latin America. *San Juan de Dios* has an area of 40 000 square metres and more than 3 000 stalls. Stakeholders report that this marketplace allegedly offers for sale a high volume of counterfeit goods, including electronic appliances, footwear, jewellery and watches as well as pirated CDs and DVDs.

The enforcement authorities have reportedly conducted several raids against rogue merchants on the market over the last two years. Stakeholders report that taking action with the support of the state authorities of Jalisco or the municipal authorities in Guadalajara remains practically impossible.

Morocco

Souk Korea, Casablanca

Stakeholder report *Souk Korea* for inclusion in the Watch List. *Souk Korea* is located in the centre of Casablanca and it is allegedly the biggest wholesale and retail marketplace for counterfeit goods in Morocco. The market allegedly offers for sale a high volume of counterfeit goods, mainly footwear, sport clothing and electronics. Stakeholders report that the majority of the goods sold on this market come from China and are stored in nearby warehouses.

Stakeholders also report that Al Wifak Association, the association that manages this marketplace, hampers enforcement by protesting against raids or moving counterfeit products to safe places before or during raids. Enforcement authorities reportedly rarely perform raids and seizures on this market and the low sanctions and soft criminal responsibility for counterfeiters do not deter infringers.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Morocco, for instance on *Jamea El Fna* in Marrakesh, on *Kissariat Attarine* in Casablanca and on *Souk Al Had* in Agadir.

Russia

Gorbushkin Dvor Mall, Moscow

Stakeholders continue reporting *Gorbushkin Dvor Mall* for inclusion in the Watch List. *Gorbushkin Dvor Mall* is located in Moscow and it is allegedly one of the biggest wholesale and retail marketplace for counterfeit goods in Russia. The *Gorbushkin Dvor Mall* is one of Russia's highest profile "tech malls". The market allegedly offers for sale

a high volume of counterfeit goods, mainly cheap consumer electronics and household appliances, but also allegedly counterfeit perfumes, clothes and fashion accessories.

Stakeholders report that enforcement in *Gorbushkin Dvor Mall* continues being almost impossible and that complaints sent by right holders are usually ignored. Obtaining evidence through covert investigations remains dangerous and the local police reportedly remains reluctant to conduct raids on any premises on this market.

The *Dubrovka Market* and *Sadovod Market* in Moscow, *Tagansky Ryad Market* in Yekaterinburg, *Market Lira* in Lviv were also reported by stakeholders for the massive amount of counterfeit goods.

Thailand

MKB Center, Bangkok

Stakeholders continue reporting *MKB Center* for inclusion in the Watch List. *MKB Center* (also known as *Mahboonkrong)* is located in Bangkok and it is allegedly one of the biggest retail shopping malls for counterfeit goods in Thailand. *MKB Center* has more than 2 000 shops and around 100-500 counterfeit goods per shop remain available with further stock places nearby. *MKB Center* allegedly offers for sale high volume of counterfeit clothing, accessories, electrical appliances (computers and cell phones), cosmetics, beauty supplies, entertainment, footwear, jewellery and watches.

The Economic Crimes Suppression Division of the Police and the Department of Intellectual Property (DIP) regularly performed surveillance over the last two years. Stakeholders report that despite these efforts, the *MKB Center* allegedly continues being home to both high and low quality counterfeit goods.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Thailand, for instance in *Rong Klua Market* in Aranyaprathet, *Patpong Night Market*, *Chatuchak Market*, *Platinum (Pratunam) Market*, *Sampeng Market*, *Maboonkrong Shopping Center*, *Tawanna Market* and *Union Mall* in Bangkok, *OTOP Market* in Phuket, *Rong Kluea Market* in Sa Kaeo, *Tachileik Market* in Mae Sai.

Turkey

Grand Bazaar, Istanbul

Stakeholder continue reporting the *Grand Bazar* for inclusion in the Watch List. The *Grand Bazar* is located in the centre of Istanbul and it is one of the biggest and oldest wholesale and retail marketplace in Turkey, allegedly selling a high volume of counterfeit goods. The *Grand Bazaar* occupies 61 covered streets and over 4 000 shops, which attract between 250 000 and 400 000 visitors daily. It is also a tourist attraction. It reportedly continues offering for sale high volume of counterfeit goods, among others counterfeit handbags, watches, cloths, perfumes, leather goods and toys.

Stakeholders report that only a few raids were performed over the last two years on this market, because it is difficult to get search warrants. Stakeholders report that most of the time the defendants are sentenced only to suspended sentences and the actions are perceived not to be sufficient to reduce the level of counterfeiting on this market.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Turkey, in particular on *Bedesten Çarşısi Market* in Izmir and on *Ak Çarşı*, in Istanbul.

Ukraine

7th km Market, Odessa

Stakeholders continue reporting the *7th km Market* for inclusion in the Watch List. The *7th km Market* is located in Odessa and it is allegedly one of the biggest retail marketplaces in Ukraine for counterfeit goods. It remains one of the largest wholesale and retail markets in Europe with 20 000 shops, pavilions, containers and warehouses and around 6 000 merchants. The 7th km Market allegedly offers for sale a high volume of counterfeit goods, mainly clothes, fashion accessories, perfumes and cosmetics. Products mainly come from China and Turkey and almost all the goods are allegedly counterfeit.

Stakeholders report that the situation has not improved considerably over the last two years because enforcement authorities reportedly hardly ever perform raids and seizures on this market. The low sanctions and soft criminal responsibility for counterfeiters do not deter infringers. The market administrators are reportedly reluctant to cooperate with right holders and to meet their requests.

The *Troyeshchyna Market* and *Khmelnitskiy Market* in Kiev and *Barabasova Market* in Kharkiv were also reported by stakeholders for the massive amount of counterfeit goods.

United Arab Emirates

Ajman China Mall

Stakeholders continue reporting the *Ajman China Mall* for inclusion in the Watch List. The *Ajman China Mall* is located in the United Arab Emirates and it is allegedly one of the biggest wholesale and retail distribution centres and transit hubs of counterfeit goods in the Middle East. *Ajman China Mall* is combined with warehouses, logistics and offices. With the occupied area of 280 000 square metres and the operating area of 100 000 square metres *Ajman China Mall* reportedly offers for sale counterfeit goods, in particular bags, shoes, watches and electrical appliances, sunglasses, perfumes and toys. Stakeholders report that the enforcement authorities are still not sufficiently active and more raids would be necessary to considerably change the situation in the *Ajman China Mall*.

Dragon Mart

Stakeholders continue reporting the *Dragon Mall* for inclusion in the Watch List. The *Dragon Mall* is located in the United Arab Emirates and it is reportedly one of the largest trading hubs of counterfeit Chinese goods outside mainland China. The 150 000-square-metre retail complex allegedly offers both at wholesaler and retailer level a variety of high and low quality counterfeit goods and currently hosts over 3 950 outlets. It reportedly provides a gateway for the supply of counterfeit products mainly targeting Middle Eastern, North African and European markets. The Dragon Mall reportedly offers for sale a wide variety of counterfeit goods, including household and electrical appliances, stationery, office appliances, communication and acoustic equipment, lamps, building materials, furniture, toys, machinery, textiles, footwear, watches and fashion accessories. Stakeholders report that several raids were conducted also over the past two

years by the enforcement authorities (in particular the Dubai Department of the Economic Development agents as well as the Dubai Police). Penalties include seizure of the products and fines, but the fines remain very low and not sufficiently deterrent according to stakeholders. Courts in the United Arab Emirates do not have authority to issue injunctions against landlords to prohibit the continuation of the IP infringements conducted by their tenants.

Jebel Ali Free Zone

Stakeholders continue reporting the *Jebel Ali Free Zone* for inclusion in the Watch List. The *Jebel Ali Free Zone* is located in Dubai and it is one of the largest regional distribution and logistics hubs of counterfeits.

Stakeholders report that counterfeiters continue using the *Jebel Ali Free Zone* to manufacture, store and especially tranship allegedly counterfeit goods to various destinations, including the European Union. According to the OECD Study on Trade in Counterfeit Goods and Free Trade Zones[171] the counterfeit goods are allegedly transhipped through Jebel Ali Free Zone in order to cleanse the documents and to camouflage the original point of production and/or departure.

Shipments arrive at the *Jebel Ali Free Zone* in big volumes and are transhipped in smaller orders to their final destination points. Goods are often relabelled or repackaged in the *Jebel Ali Free Zone*. Consequently, in most cases it is difficult for customs officers to determine the country of origin, because of document cleansing[172] and also because the actual process of counterfeiting may not take place in the same country as the production of a given good.

The *Karama Shopping Complex*, the *Islamic Souk*, the *Souk Naif, the Global Village* and *Gold Souq* in Dubai and *Bengali Garments Market* in Ajman were also reported by stakeholders for the massive amount of counterfeit goods.

Vietnam

Saigon Square Plaza, Ho Chi Minh City

Stakeholders continue reporting the *Saigon Square Plaza* for inclusion in the Watch List. The *Saigon Square Plaza* is located in Ho Chi Minh City and it is one of the largest retail markets in Vietnam, allegedly offering for sale a high volume of counterfeit goods, in particular clothes, fashion accessories, shoes, phone accessories, cosmetics, beauty supplies, electronic appliances, jewellery and watches.

Stakeholders report that the situation has not improved over the past two years because the enforcement authorities only occasionally conduct raids in this plaza, thus the high level of counterfeiting reportedly persists.

The *Lucky Plaza, An Dong Market, Binh Tây Market, Kim Biên Market, Dan Sinh Market* and *Ben Thanh Market* in Ho Chi Minh City, *Dong Xuan Market, Cho Troi*

[171] OECD Study on Trade in Counterfeit Goods and Free Trade Zones - https://www.oecd.org/gov/trade-in-counterfeit-goods-and-free-trade-zones-9789264289550-en.htm

[172] See footnote 25.

Market, Son Long Shopping Mall, Ninh Hiep Market in Hanoi were also reported by stakeholders for the massive amount of counterfeit goods.