EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

VENDOR ACCOUNTS ON THIRD PARTY TRADING PLATFORMS

RESEARCH ON ONLINE BUSINESS MODELS INFRINGING INTELLECTUAL PROPERTY RIGHTS – PHASE 4

Report

October 2021

ISBN 978-92-9156-298-5 doi:10.2814/279240 TB-09-21-391-EN-N

Contents

FOREWORD 6

EXECUTIVE SUMMARY 8

INTRODUCTION AND METHODOLOGY 19

1. ONLINE IP INFRINGEMENT ON THIRD PARTY TRADING PLATFORMS 21

1.1 DEFINING THE PROBLEM 21

1.1.1 The global counterfeit market and its impact on EU economy 21

1.1.2 Online enforcement and international cooperation 26

1.1.3 Risks to consumers 26

1.1.4 Liaisons with other criminal activities 27

1.1.5 Emerging trends 29

1.2 BUSINESS MODEL ANALYSIS 32

1.2.1 Infringing goods 33

1.2.2 Online marketplaces 41

1.2.3 Darknet marketplaces 45

1.2.4 Marketplace types and categories of infringing goods 46

1.3 THE IP INFRINGEMENT SUPPLY CHAIN 48

1.3.1 Introduction 48

1.3.2 Raw material supply 51

1.3.3 Production 52

1.3.4 Storage and inventory 53

1.3.5 Online offer of sale 55

1.3.6 Marketing 57

1.3.7 Sales 60

1.3.8 Shipping 62

2. ENFORCEMENT AGAINST INTELLECTUAL PROPERTY INFRINGEMENTS ON THIRD PARTY TRADING PLATFORMS 64
2.1 MEASURES, POLICIES AND TACTICS 64
2.1.1 Proactive measures 64
2.1.2 Reactive measures 69
2.1.3 Investigation and enforcement 74
2.2 VENDORS' LIABILITY: SELECTED CASE-LAW FROM EU MEMBER STATES 84
2.2.1 Sale of pirated software on an auction marketplace 85
2.2.2 Sale of counterfeit spare parts and pirated diagnostic software on an auction marketplace 88
2.2.3 Sale of counterfeit clothing on an auction marketplace 89
2.2.4 Sale of counterfeit luxury goods from an online shop 91
2.2.5 Sale of pirated design articles on an auction marketplace 92
2.3 INJUNCTIONS AGAINST INTERMEDIARIES 94
2.3.1 Legal basis for injunctions against intermediaries 95
2.3.2 Primary and secondary liability for trade mark infringement 97
2.3.3 e-commerce exemptions from liability 99
2.3.4 Injunctions to prevent further infringements 103
2.3.5 Allocations of costs of injunctions 105
2.4 JURISDICTION OF IP INFRINGEMENT CASES 106
2.4.1 Conflict of law in online infringement of national trade marks 109
2.4.2 Conflict of law in online infringement of EU trade marks 110
2.4.3 Conflict of law in online infringement of copyright and related rights 112
2.4.4 Conflict of law in online infringement of Community designs 113
2.4.5 International disputes with undertakings domiciled in non-EU Member States 114
2.4.6 Recognition and enforcement of foreign judgments 116
2.4.7 Criminal jurisdiction 119

Conclusion 120

APPENDIX: Case studies 123

FOREWORD

Today, shopping online is an everyday task. Online trading platforms are used by billions of users, large and small businesses around the world, to make all kind of products available for purchase at a click of a button. They have opened up new market opportunities and brought e-commerce within easy reach for everyone.

However, platforms can be misused by vendors who use their services to import, sell and distribute goods that infringe intellectual property. The market for counterfeit and pirated goods is on the rise too, following the same pattern as global commerce and shifting from physical to online distribution. With the rise of the darknet, new means of infringing intellectual property have emerged.

In 2011, the European Commission facilitated a Memorandum of Understanding (MoU) to hinder the sale of counterfeit goods on online marketplaces. Under this voluntary agreement, revised in 2016, rights owners, internet platforms and associations defined a series of joint practices to prevent offers of counterfeit goods from appearing on online marketplaces.

To give full effect to such voluntary practices, as well as to customs controls, law enforcement actions and criminal prosecutions, a methodical knowledge of the 'business models' underlying IP infringements is needed.

The EUIPO is working with IP stakeholders and a number of platforms to improve trade mark protection in online marketplaces, and to combat counterfeiting generally. However, this is a complex area requiring a detailed understanding of the tactics, techniques and procedures used by vendors of counterfeit and pirated goods via vendor accounts.

This report fills a gap in the knowledge of the tactics, techniques and procedures used by vendors on third-party trading platforms. It provides a systematic understanding of the various stages of the 'supply chain' of infringing goods online, and of the enforcement actions that can be deployed at each

stage. It also unveils emerging forms of marketing of IP-infringing goods through social media and live streaming, which pose new challenges to investigators and law enforcers.

The research clarifies that the supply of counterfeit and pirated products via online marketplaces is a lucrative and highly organised activity that can only be tackled through global cooperation, and if it is a focus priority of law enforcement actions. The research casts light into a hidden dimension of international e-commerce which endangers economic operators and consumers alike, and should help raise awareness among EU and third-country citizens, businesses, authorities and policy makers.

The report comes at a very pertinent moment as the Council of the EU recently adopted conclusions setting the 2022-2025 EU priorities for the fight against serious and organised crime through the European Multidisciplinary Platform against Criminal Threats (EMPACT) that will include intellectual property crime.

EXECUTIVE SUMMARY

Background

In 2020, the European Union Intellectual Property Office (EUIPO), through the European Observatory on Infringements of Intellectual Property Rights, commissioned a research study on intellectual property (IP) infringement through vendor accounts on third-party trading platforms. The purpose of the research was to enhance the level of understanding about the ways in which IP infringers misuse online trading platforms to market goods and services infringing IP rights, how the business models adopted by IP infringers work, and thereby provide new knowledge to tackle the challenge of this phenomenon more effectively.

The research study was commissioned to the Centre for Intellectual Property Policy and Management (CIPPM) of Bournemouth University, which set up a team of researchers in law and computer science ([1]). The research team was assisted by a group of experts including representatives of rights holders, online trading platforms, shipping and payment companies, law enforcement, judiciary, private investigation services and digital security.

This report was carried out as a study into the legal, technical and logistical aspects of the supply of IP-infringing goods and services on online trading platforms. It reviews the existing literature and policy initiatives, the legislative framework and case-law and provides a qualitative analysis of the existing business models and the available enforcement options to respond to them.

([1]) Bournemouth University research team was led by Professor Maurizio Borghi and Professor Vasilis Katos, and included Dr Dimitrios Koukiadis, Dr Cagatay Yucel, Mr Panagiotis Bellonias, Mr Ioannis Chalkias and Mr Dukki Hong.

Methodology

The business models analysis was developed through a series of structured interviews with domain experts and an independent investigation leveraging cybersecurity techniques. A series of structured interviews was carried out with experts representing brand owners, rights holders, online marketplaces, customs, courier services, payment service providers, judiciary and law enforcement. Independent research was carried out using cybersecurity investigation approaches and practices in the domain of digital forensics and incident response. Such an approach allowed the identification of the so-called tactics, techniques and procedures (TTPs) used by the infringers. The TTPs were then developed in the business case descriptions and formed the basis of the analysis of the business models ([2]).

The context of the study: IP infringement in a changing internet environment

In 2019, the value of counterfeit and pirated goods imported in the EU was estimated to be **up to EUR 119 billion, or 5.8 % of all EU imports** ([3]). Internet transactions account for a major share of this value. The huge market penetration of online trading platforms makes them a sought-after channel for the sale of those goods. As highlighted by the EUIPO and Europol in 2019, the misuse of these platforms has become 'an important source of income for criminal groups engaged in the sale of counterfeit and pirated goods' ([4]).

While the sale of infringing goods on online marketplaces is not new, some **emerging trends** hamper IP enforcement efforts.

- **Multiple vendor accounts**. Organised crime groups (OCG) systematically misuse trading platforms by opening multiple accounts under different names on the same platforms and across different media.

([2]) A selection of 13 case studies is presented in Appendix to this report.

([3]) OECD/EUIPO (2021) *Global Trade in Fakes: A Worrying Threat*, OECD Publishing, Paris 2021, p. 3 and 58.

([4]) EUIPO/Europol (2019) *Intellectual Property Crime Threat Assessment 2019*, p. 11.

- **Online advertising**. Vendors manipulate online advertising services by associating their illicit activity with brands, and place adverts on legitimate websites or social media platforms to direct traffic to external websites or to online marketplaces' listings offering IP-infringing goods.

- **Social media presence.** Vendors can misuse multiple functionalities of social media platforms to reach a high number of consumers ([5]). For example, they can advertise counterfeit goods through posts and messages via public, private or selected group communication, or through live-streaming sales, and then direct customers to illegal sales, either on external platforms or on the social media e-commerce facilities.

Mapping IP infringements on online trading platforms

IP-infringing activities occurring on online marketplaces involve primarily the sale of counterfeit or pirated goods. Counterfeit and pirated goods are defined in various legal instruments and national legislations. These definitions may vary significantly. For the purpose of this study, counterfeit refers to a blatant form of trade mark infringement, where goods bear a sign that is either identical or otherwise indistinguishable from a registered trade mark. Counterfeit goods range from low-quality imitations ('fakes') to copies that are closer to the appearance of branded products ('replicas'). Piracy is the sale of goods that infringe copyright or design rights, and it applies to both physical and digital goods.

Other forms of IP infringement involve the use of signs that are confusingly similar to those of the legitimate trade mark owner, or that cause harm to a trade mark's reputation. These less blatant forms of infringement encompass both simple and very complex cases, which may require ad hoc examination. Furthermore, IP infringement may involve the sale of 'grey market' products, namely authentic products that are imported and sold without the authorisation of the IP owner.

([5]) EUIPO (2021) *Monitoring and analysing social media in relation to IP infringement*; EUIPO (2021) *Social Media – Discussion Paper. New and existing trends in using social media for IP infringement activities and good practices to address them*, June 2021.

For the purposes of the present study, the descriptions as appear in the following table are used. These descriptions may differ from the purely legal definitions in some jurisdictions, but the idea is that all the activities or goods covered violate IPRs in a way or another.

	INFRINGING GOODS: EXAMPLES	
	Physical	Digital
Counterfeit	• Fakes (low-quality imitations) • Replica (same-appearance copies)	• Computer Aided-Design (CAD) files for 3D printing
Piracy	• Copies of copyright content on physical support (CD, DVD) • Replica design objects • TPM circumvention devices • TV decoder smartcards • Fully-loaded set-top boxes or sticks	• Software copies • Activation keys for software, video games or databases • Hacked accounts for streaming services • Computer Aided-Design (CAD) files
Confusion	• Look-alike brand name, logo or packaging on similar goods	• Look-alike brand name and/or logo on similar digital goods, e.g. software, video games or apps
Brand exploitation	• Use of famous brands on unrelated goods	• Use of famous brands in virtual worlds or on non-fungible tokens
Grey market	• Parallel imports • Overruns • Rejects	n/a

The IP infringers' choice of the online platform is highly dependent on the kind of good or service that is offered for sale, the target audience and whether the infringer is an 'occasional' or 'systematic' vendor. Alongside 'general' wholesale and auction marketplaces there are 'specialised' marketplaces, such as marketplaces for handcrafted goods, independent retailers, digital goods (e.g. video games and software licences) and non-fungible tokens (NFT). An increasingly important role is played by 'social commerce', namely C2C and B2C sales through social media. Major social media platforms have developed their own e-commerce functionalities. A growing trend is the use of social media live-streaming facilities to market and demonstrate the product to buyers.

Systematic counterfeit sellers may also use illegal marketplaces operating in the darknet, where transactions are carried out anonymously and using cryptocurrencies.

The table below illustrates indicatively the **destination marketplaces** for each category of IP-infringing goods, in terms of likelihood that a given product is detected on a certain type of marketplace.

Marketplace type	Infringing goods: I. Counterfeit	II. Piracy	III. Confusion	IV. Exploitation	V. Grey-market
Wholesale					
Auction/2nd hand					
Handcraft / art					
Social Media					
Labour / Services					
Digital goods					
Darknet					

A supply-chain approach to investigation and enforcement

The process underlying IP infringements via vendor accounts on third-party trading platforms consists of a seven-stage supply chain, from the production to the delivery of the infringing good. It is a continuous process through a flow of information, physical items and money that involves a number of intermediaries. From an enforcement perspective, the visibility of the illegal activity is expected to decrease as we travel back along the supply chain (from right to left) and to increase as we approach the customer (shipping, at the far right).

Along the supply chain, **infringers** use a number of techniques to elude enforcement actions, such as techniques to elude detection, takedown, seizure or confiscation of goods. This informs the actions that can be taken by **enforcement actors** at each stage of the chain. These actions include investigation and law enforcement, as well as self-regulatory enforcement measures.

The table below summarises the **key enforcement actions** available to law enforcers, online platforms and IP owners at each stage of the supply chain:

	ENFORCEMENT ACTIONS
	• **Monitoring of materials:** identification of hotspots where the materials are produced or originate from and maintaining a database of locations. • **Custom checks:** leverage historical information from countries of origin and/or known hotspots and information on custom declaration forms.
	• **Blocking the bank accounts** of the producers. • **Following trends** and seasonal events that affect the production of goods (e.g. beginning of sport events, release of popular products).
	• **Confiscation/seizure of goods**: raiding the inventory of IP infringers and taking control of the infringing items.
	• **Detection** of the vendors of the illicit items that are hosted, unknowingly, by the trading platform. • **Activation of notice-and-takedown procedures**: taking down listings and vendor accounts.
	• **Following flags**: alert indicators for a marketplace, such as offers that are: 'too good to be true' and/or receive an inflated amount of positive feedback in a short time. • **Monitor communication**: follow online communications from social media platforms, peer-to-peer communication and ad applications. • **Advertisement takedowns**: takedowns of ad keywords, de-listing results on search engines, removal of a product or vendor account.
	• **Liaison with banks/financial authorities** to detect and identify the entities behind financial transactions and block bank accounts. • **Liaison with payment service providers** to block transactions in the case of identified illicit vendors. • **'Follow-the-money' investigations**: create a full profile of the vendors by analysing the financial transactions under investigation. • **Test purchases**: purchasing of IP-infringing products to collect the evidence required to build a case against an illicit vendor.
	• **Liaison with couriers/postal services** to prevent the distribution of counterfeit products and/or identify the distributors' addresses.

	• **Liaison with customs** to activate procedures for seizure and forfeiture of infringing goods and request data after goods are destroyed. • **Seizure of goods** at customs or postal services. • **Monitoring routes** to discover the origin of the product, distributors and vendors and how the products are transferred to the buyers. • **Monitoring suspects** who receive unusual amounts of unexpected orders from regular routes.

Measures, policies and strategies for effective enforcement

Tackling IP infringements on third-party trading platforms involves a number of measures, policies and tactics. These include enforcement actions and voluntary measures taken as part of the collaboration between all stakeholders involved. In the EU, the MoU, signed in 2011 and revised in 2016, provides the general framework for these voluntary measures ([6]). Good practices under the MoU include **proactive measures** aimed at preventing infringing activities before they occur, and **reactive measures** aimed at repressing or limiting the effect of those activities once they occur.

- **Voluntary proactive and preventive measures (PPM)**. The legal basis for these measures is provided by the contractual obligations deriving from the acceptance of the Terms & Conditions (T&C) of online marketplaces, which prohibit the sale of goods that infringe third parties' rights. These measures, developed in collaboration with IP owners, include the following.

  (i) **Repeat offenders policies**: users that repeatedly violate the T&C may have their accounts suspended or disabled.

  (ii) **Identity verification**: to ensure effectiveness of policies against repeat infringements, platforms require users to provide valid identification, such as proof of identity or an

([6]) European Commission (2016) *Memorandum of understanding on the sale of counterfeit goods on the internet*, https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en.

address, as a condition for opening an account. Trading platforms may also require proof of a business licence and may restrict the use of certain keywords in profile names.

(iii) **Traceability of products**: major trading platforms have introduced traceability schemes in which each item is provided with a unique code to verify its authenticity before it reaches the customer.

(iv) **Other technological prevention measures**: trading platforms and social media apply keyword filtering, content moderation and image recognition technology to detect infringing listings before the sale can be finalised.

- **Notice-and-takedown (NTD)**: NTD procedures represent the key voluntary **reactive measures** to streamline the process of notification and removal of infringing content that is made available online. According to the good practices developed in the framework of the MoU, effective NTD procedures include the following.

(i) **information package for rights holders**, with detailed instructions on the information that must be submitted to activate the notification.

(ii) tools to manage **multiple notifications**, or 'in-bulk' requests, enabling rights holders to include multiple infringing listings in a single takedown request.

(iii) **'trusted flaggers' programmes**, with fast-track, privileged channels for notifications and more expeditious removal for 'trusted' rights holders with specialised expertise and dedicated technology for the detection and identification of infringing content.

(iv) **search and report tools**, to facilitate the process of searching for potentially infringing content on the platform, by means of image recognition and other technologies.

(v) **information for users** on the reason for the removal and the potential consequences of repeated infringements, as well as easily accessible information on the right to appeal or **counter-notice procedure** to challenge the notice of the IP owner.

- **Automated detection measures**. Detection systems based on artificial intelligence and machine learning play an increasing role in both proactive and reactive measures.

Along with the voluntary measures developed in collaboration with online marketplaces, rights holders and law enforcement agencies adopt investigative and enforcement measures that are broader in scope and span across the whole supply chain.

- **Follow-the-money investigation.** A 'follow-the-money' approach consists in monitoring and extracting information from the financial transactions involved in an illicit activity, with the purpose of collecting evidence and/or disrupting the activity. The approach requires cooperation between the different stakeholders involved, most importantly the payment services, and has been adopted in proceedings against IP infringers.

- **Customs and border checks.** EU customs authorities adopt streamlined procedures and condensed time frames to destroy suspected IP-infringing goods in small packages, and provide data to rights holders on request.

- **Darknet enforcement.** Given the anonymity of online providers and possible affiliates, enforcement in the darknet marketplaces presents specific challenges. Global cooperation between law enforcement authorities has led to the **shutdown** of darknet marketplaces.

Vendors prosecution

Legal actions can be taken against vendors for importation, offer for sale and distribution of IP-infringing goods. Proceedings can be brought by IP owners or by operators of online marketplaces, or jointly by both. While civil liability for IP infringement is broadly harmonised at EU level, at least as far as direct infringement is concerned, criminal liability remains the competence of national legislators. In most EU Member States, the infringement of trade marks or copyright and related rights attracts criminal sanctions when the infringer acts with *mens rea* or wilful intent and on a commercial scale. However, these criteria are not construed uniformly across Member States.

There is limited evidence of legal proceedings against individual vendors in the EU-27. The available case-law suggests that **wilful intent** can be established based on objective factors, such as a lack of

express authorisation from the trade mark owner or constructive knowledge that the products are counterfeit. The criterion of **'commercial scale'** is less clear, and heavily dependent on the volume of transactions. Evidence of activity such as receiving orders and shipping is crucial to determine the volume required by national jurisdictions to trigger criminal sanctions.

Injunctions against intermediaries

Together with legal actions against vendors, IP owners may seek remedies from the operators of online marketplaces and other intermediaries along the supply chain. These include, in particular, warehouses, advertising platforms, payment services and shipping services. The judicial remedies available consist of **injunctive relief**, which may be granted by the judicial authority even when the intermediary is not liable for the infringement or is exempt from liability.

Injunctions against intermediaries can aim not only at terminating existing infringements but also at preventing further infringements. This requires the implementation of some proactive monitoring duties. The scope of such monitoring duties under EU law is limited by the provisions of the e-Commerce Directive ([7]) and can be derived from the **'double identity' approach** suggested by Advocate General Jääskinen in the 'L'Oréal v eBay' case: 'the infringing third party should be the same and that the trade mark infringed should be the same in the cases concerned' ([8]).

The issue of jurisdiction

Due to the transnational nature of IP infringements committed through vendor accounts on third-party marketplaces, the issue of jurisdiction is a crucial aspect for effective enforcement. Claimants are generally obliged to bring a case before the courts where the defendant is **domiciled**, but it is also possible to start proceedings in the place where the **damage** occurred, where the **event** that caused the damage took place, or where the infringement was **committed**.

([7]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Article 15(1).
([8]) Opinion of AG Jääskinen (12/07/2011, C-324/09, L'Oréal SA-eBay, EU:C:2010:757, § 182).

In relation to the allocation of jurisdiction in civil proceedings, a key factor to consider is whether the infringers targeted the EU (in the case of **pan-EU IP rights**) or a specific Member State. If the target is established, IP owners may bring proceedings before the courts of the targeted jurisdiction.

IP RIGHTS	LEGAL BASIS TO ESTABLISH JURISDICTION IN INTERNATIONAL (PAN-EU) IP DISPUTES
EU trade marks	EUTM Regulation No 2017/1001 ([9]), Article 125
Community designs	Community Designs Regulation No 6/2002 ([10]), Article 82
National IP rights (national trade marks, copyright and related rights, patents, etc.)	Brussels I Regulation (recast) ([11])

Recognition and enforcement of **foreign judgments** between EU Member States is uniformly provided by the Brussels I Regulation (recast), whilst enforcing judgments in jurisdictions other than EU Member States can be extremely challenging due to the discrepancies in national laws.

Jurisdiction in **criminal law matters** is generally based on the **principle of territoriality**. Currently, there are no binding instruments under EU law to resolve conflicts of jurisdiction in criminal matters. However, the Council of Europe Cybercrime Convention 2001 ([12]) represents an important instrument of international law that assists in determining adjudication in criminal proceedings against online copyright infringers ([13]).

([9]) Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark, OJ L 154, 16.6.2017, p. 1.

([10]) Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, as amended, OJ L 386, 29.12.2006, p. 14.

([11]) Regulation (EU) 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351, 20.12.2012, p. 1.

([12]) Convention on Cybercrime, European Treaty Series No 185.

([13]) EUIPO (2021) *International judicial cooperation in intellectual property cases*, March 2021, p. 33.

INTRODUCTION AND METHODOLOGY

This report surveys the legal and logistical aspects of Intellectual Property (IP) infringement through misuse of legitimate services offered by online trading platforms. It covers IP infringements involving both physical and digital products offered for sale through vendor accounts on a range of online platforms and provides a structural analysis of existing business models and available enforcement actions for the entire 'supply chain' for those products. The business model analysis ranges from well-known forms of sale via accounts on marketplace platforms, to emerging techniques featuring social media presence and live-streaming sales.

For the purpose of this report, the following definitions are adopted.

- **Third-party trading platforms** are online platforms where registered users and businesses offer goods or services for sale to other users or businesses. E-commerce stand-alone websites are not included here. The study covers platforms operating both on the surface web and the darknet ([14]).

- **Vendor accounts** are user accounts created on trading platforms and social media with the purpose of offering goods or services for sale. They include business-to-consumer (b2c) as well as consumer-to-consumer (c2c) and business-to-business (b2b) illegal activities.

- **IP infringement** includes any use of IP rights not authorised by the rights holder or covered by statutory exemptions (such as exhaustion of rights). Accordingly, the study covers the sale of counterfeit and pirated goods and of confusingly similar infringing goods, as well as the sale of authentic goods without the rights holder's authorisation ([15]). Other illegal activities that may be

([14]) section 1.2.2 and 1.2.3.

([15]) section 1.2.1.

perpetrated by third parties misusing online trading platforms, such as scams, fraud and ID theft, are outside the scope of the study.

Methodology

The study applied desk-based research and comparative legal analysis, coupled with qualitative interviews with experts and independent research of selected business case studies using cyber security investigation techniques.

The study is based on an extensive review of the existing literature, initiatives and resources relevant to the object of the study. In addition, the study applied comparative analysis of the key legal issues in relation to IP infringement through online trading platforms, namely liability, jurisdiction and enforcement. While the focus of the analysis is the EU-27, the study also considers, from a comparative perspective, the approaches in other non-EU jurisdictions. A selection of case-law on IP infringement through the misuse of online trading platforms has also been included.

The approach adopted for the research on the business cases in this report was informed by two main activities. First, a series of structured interviews were conducted with domain experts. These experts covered all aspects of the supply chain (brand holders and other rights owners, courier services, and the marketplaces themselves) as well as independent investigators, legal experts, law enforcement officers and members of the judiciary. Second, the analysis leveraged cybersecurity investigation approaches and practices, particularly those used in the domain of digital forensics and incident response. This approach allowed the identification of the infringers' so-called Tactics, Techniques and Procedures (TTPs). The TTPs were then elaborated in the business case descriptions and informed the analysis of business models.

1. ONLINE IP INFRINGEMENT ON THIRD PARTY TRADING PLATFORMS

1.1 DEFINING THE PROBLEM

1.1.1 The global counterfeit market and its impact on EU economy

In an innovation-driven global economy, infringements of intellectual property rights (IPR) – in particular commercial-scale counterfeiting and piracy – pose a major problem for the global economy and the European Union (EU) in particular. IP infringements cause high financial losses for European rights holders and sustainable IP-based business models. The EU has a particular interest in IP enforcement, given that European companies are leading providers of IP-protected goods and services in third countries' markets ([16]).

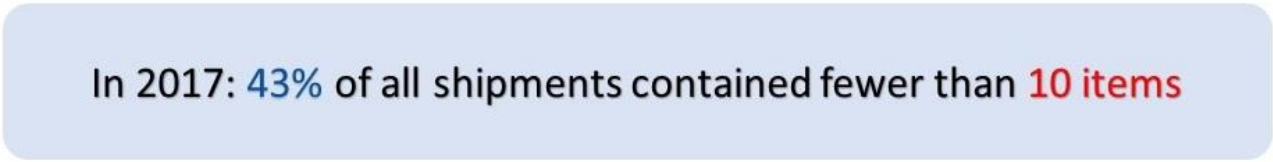
The ways in which consumers enjoy physical products – such as clothing, cosmetics, accessories, electronic devices, pharmaceutical products – and digital content – such as music, films, e-books and video games – have changed drastically over the past 15 years. The internet has become the main means of distribution, not only for digital content but also, increasingly, for physical goods, with e-commerce sales steadily rising compared to 'bricks-and-mortar' sales ([17]). Counterfeiting and piracy have followed the same pattern, and have shifted from physical to online distribution ([18]). Moreover, the data shows that small shipments and parcels tend to dominate numerous trade routes, reflecting the shrinking costs of postal and courier shipments and the increasing importance of internet and e-commerce in international trade. In 2017 it was estimated that shipments with fewer than ten items

([16]) *IPR-intensive industries and economic performance in the European Union*, EPO/EUIPO, third edition, September 2019.

([17]) In the EU-27, the enterprise turnover generated from e-sales increased by 7 % in nine years, namely from 13 % in 2010 to 20 % in 2019 (*E-commerce statistics explained*, Eurostat, 01/03/2021, https://ec.europa.eu/eurostat/statistics-explained/pdfscache/14386.pdf)

([18]) The legal definition of counterfeit and piracy is discussed in section 1.2.1.

accounted for about 43 % of all shipments, on average ([19]). Data also shows that, between 2014 and 2016, a large majority (57%) of seizures of counterfeit and pirated goods worldwide concerned postal parcels. However, in terms of value of those customs seizures, over a half (56%) concerned maritime shipments via containers ([20]).



Over the years, a variety of private and public organisations have attempted to estimate the size and value of the international market for counterfeit goods from an international and comparative perspective. A study commissioned by the U.S. Patent and Trademark Office found figures ranging from USD 200 billion (EUR 165 billion) in 2008 to USD 509 billion (EUR 420 billion) in 2019 ([21]). As of 2018, counterfeiting was the largest criminal enterprise in the world, with domestic and international sales of counterfeit and pirated goods totalling between an estimated USD 1.7 trillion (EUR 1.4 trillion) and USD 4.5 trillion (EUR 3.7 trillion) a year – higher than either drugs or human trafficking ([22]). Around

([19]) OECD/EUIPO (2017) *Mapping the Real Routes of Trade in Fake Goods*, OECD Publishing, Paris 2017, available at http://dx.doi.org/10.1787/9789264278349-en.

([20]) OECD/EUIPO (2021) *Misuse of Containerized Maritime Shipping in the Global Trade of Counterfeits*, OECD Publishing, Paris 2021, available at https://doi.org/10.1787/26175835, p. 40-41.

([21]) *U.S. Intellectual Property and Counterfeit Goods, Landscape Review of Existing/Emerging Research,* A Report Prepared by the Federal Research Division, Library of Congress, under an Interagency Agreement with the U.S. Patent and Trademark Office, U.S. Department of Commerce, April 2020.

([22]) *U.S. Intellectual Property and Counterfeit Goods, Landscape Review of Existing/Emerging Research,* A Report Prepared by the Federal Research Division, Library of Congress, under an Interagency Agreement with the U.S. Patent and Trademark Office, U.S. Department of Commerce, April 2020.

80 % of these goods are produced in China, and 60 % to 80 % of those products are purchased by American citizens ([23]).

In April 2016, the EUIPO and the Organisation for Economic Co-operation and Development (OECD) jointly published the report *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact* ([24]). The report was based on seizure data from the World Customs Organisation, DG TAXUD (Directorate-General for Taxation and Customs Union) and the US Customs and Border Patrol. According to the report, in 2013, international trade in counterfeit products represented up to 2.5 % of world trade, equivalent to up to USD 461 billion (EUR 338 billion) ([25]). This constituted an increase compared to the first such study carried out by the OECD in 2008 and updated in 2009, which showed global trade in counterfeits of up to USD 250 billion (EUR 200 billion), or 1.9 % of world trade. However, it must be acknowledged that the 2016 study reflects significant improvements in the methodology and data used, so care must be taken when comparing the two figures. Subsequent updates to the report showed a sustained level of trade in counterfeit and pirated goods globally, with an estimate of up to 3.3% of world trade in 2016, or USD 509 billion (EUR 373 billion) ([26]), and up to 2.5 % of world trade in 2019, or USD 464 billion (EUR 340 billion) ([27]).

Size of global trade in counterfeit and pirated goods in 2019

Up to USD 464 billion (EUR 340 billion)

2.5 % of world trade

([23]) *U.S. Intellectual Property and Counterfeit Goods, Landscape Review of Existing/Emerging Research,* A Report Prepared by the Federal Research Division, Library of Congress, under an Interagency Agreement with the U.S. Patent and Trademark Office, U.S. Department of Commerce, April 2020.

([24]) OECD/EUIPO (2016) *Trade in Counterfeit and Pirated Goods. Mapping the Economic Impact*, OECD Publishing, Paris 2016, p. 11.

([25]) OECD/EUIPO (2016) *Trade in Counterfeit and Pirated Goods. Mapping the Economic Impact*, OECD Publishing, Paris 2016, p. 11 and 76.

([26]) OECD/EUIPO (2019) *Trends in Trade in Counterfeit and Pirated Goods*, OECD Publishing, Paris 2019, p. 11 and 45-46.

([27]) OECD/EUIPO (2021) *Global Trade in Fakes: A Worrying Threat*, OECD Publishing, Paris 2021, p. 8 and 52-53.

More specifically, the value of counterfeit and pirated goods imported into the EU in 2013 was estimated to amount to as much as EUR 85 billion, or 5 % of total imports: a relative impact on imports which was twice as high as on a world scale. Applying the same methodology, the follow-on report of 2019, estimated that the value of counterfeit and pirated imports in the EU rose to up to EUR 121 billion in 2016, corresponding to 6.8 % of all EU imports ([28]). The latest follow-on report of 2021 shows substantially similar figures for 2019, with up to EUR 119 billion or 5.8% of all EU imports ([29]).

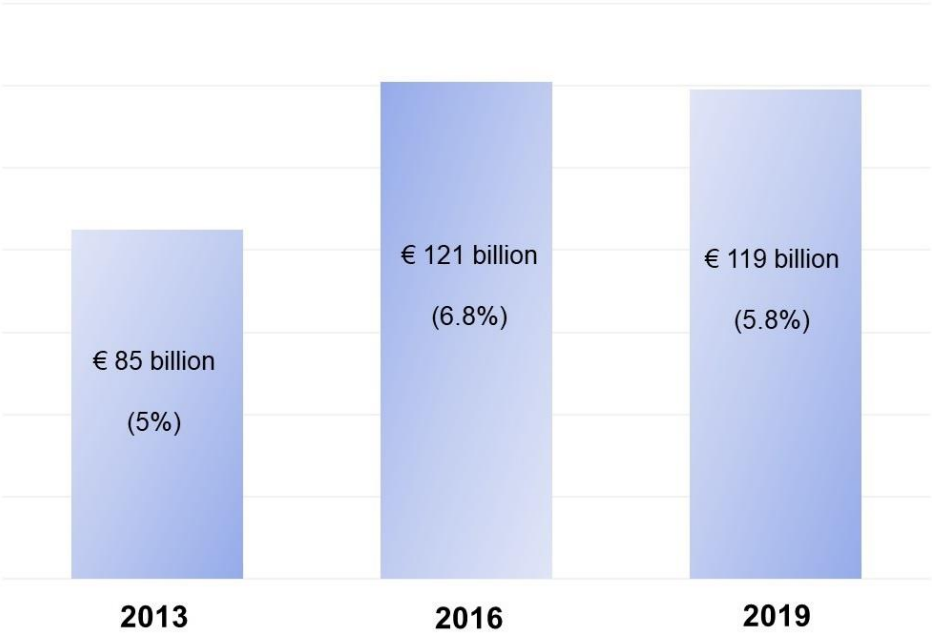


Figure 1 – Estimated value of imports of counterfeit and pirated goods in the EU, and percentage of total EU imports

This phenomenon has both direct and indirect impact on the EU economy as a whole. In a study carried out in partnership with the European Patent Office (EPO), the EUIPO estimated that the total contribution of IPR-intensive industries to the EU economy in the years 2014-2016 accounted for approximately 45 % of GDP (EUR 6.6 trillion annually) and 29 % of employment (plus another 10 % in

([28]) OECD/EUIPO (2019) *Trends in Trade in Counterfeit and Pirated Goods*, OECD Publishing, Paris 2019, p. 14 and 57.
([29]) OECD/EUIPO (2021) *Global Trade in Fakes: A Worrying Threat*, OECD Publishing, Paris 2021, p. 3 and 58.

indirect employment effects in non-IPR intensive sectors) ([30]). Those sectors also generate a trade surplus of approximately EUR 166 billion in the rest of the world and pay their workers 47 % higher salaries than other sectors ([31]).

IPR-intensive industries in the EU

45 % GDP (EUR 6.6 trillion annually)

29 % of employment

Given these numbers, and the consequent high value associated with IPR, it is plain to see why the online sale of counterfeit and pirated products has become such a lucrative criminal activity, generating significant costs, not only for the rights owners, but also for the economy in general. **The EUIPO has considered lost sales in 11 sectors to the value of over EUR 83 billion per year** ([32]).

Furthermore, it was revealed that whilst 97 % of Europeans surveyed believed that IP was important in protecting the rights of inventors and creators, 10 % had purchased counterfeit goods, and a similar proportion admitted to having intentionally downloaded or streamed content from illegal online sources during the previous 12 months ([33]). This shows that both the price and the availability of these goods and services play a crucial part in the decision-making process.

([30]) EPO/EUIPO (2019) *IPR-intensive industries and economic performance in the European Union*, third edition, September 2019.

([31]) EPO/EUIPO (2019) *IPR-intensive industries and economic performance in the European Union*, third edition, September 2019, p. 4.

([32]) EUIPO (2020) *Status Report on IPR Infringement*, June 2020.

([33]) EUIPO (2017) *European Citizens and Intellectual Property: Perception, Awareness, and Behaviour*, March 2017, p. 7 and 11.

1.1.2 Online enforcement and international cooperation

The abovementioned numbers show that the online sale of counterfeit and pirated goods is important for enforcement and police authorities worldwide, and features in the crime areas of EU and international cooperation agencies such as Europol, Eurojust and Interpol ([34]). In its role as a forum in which governments can work together to share experiences and seek solutions to common problems, the OECD has published several reports on counterfeiting and piracy, focussing globally and on national economies ([35]). The EU Taxation and Customs Union facilitates collaboration with national customs authorities in the fight against counterfeiting in the European Union ([36]). Another network involved in this area is the Consumer Protection Cooperation (CPC) Network. This network was also created by the European Commission, and it comprises authorities that can act on infringements of consumer legislation. They carried out a major sweep in 2014, checking websites that were active on EU territory ([37]).

A review of the enforcement measures available in relation to the sale of IP-infringing goods through online marketplaces is presented in part 2 ([38]).

1.1.3 Risks to consumers

In March 2017, the European Consumer Centre (ECC-Net) published the report *The impact of counterfeiting on online consumer rights in Europe* ([39]), focusing on the risks of buying counterfeits on the internet, and giving tips for consumers in Europe who want to avoid unpleasant surprises due to

([34]) 'Intellectual property crime', Europol (https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/intellectual-property-crime); 'Illicit goods', Interpol (https://www.interpol.int/Crimes/Illicit-goods).

([35]) EUIPO/OECD series *Illicit trades* (https://www.oecd-ilibrary.org/governance/illicit-trade_26175835).

([36]) www.ec.europa.eu/taxation_customs/home_en.

([37])www.ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm#maincontentSec3.

([38]) section 2.1.

([39]) European Consumer Centre Ireland (2017) *The impact of counterfeiting on online consumer rights in Europe. The risks of buying counterfeits on the Internet, and tips from the ECC-Net for consumers in Europe who want to avoid unpleasant surprises due to these products,* March 2017, available at https://www.eccireland.ie.

buying counterfeit products. Moreover, the report deals with the impact of counterfeiting on individual consumers who shop online, and who may encounter counterfeit goods in this way.

The relationship between counterfeit and dangerous or unsafe goods has been investigated by the EUIPO in the *Qualitative study on risks posed by counterfeits to consumers*, published in June 2019. The study reviews the data from the European Commission's "Rapid Alert System for dangerous non-food products" (RAPEX), that is the online system used by EU market surveillance authorities to report unsafe products found on the internal market ([40]). The analysis of RAPEX alerts over seven years shows that 97% of reported dangerous counterfeit products were assessed as posing "serious risk", with the most common dangers related to exposure to hazardous chemicals and toxins, poorly constructed products, and use of inferior supplies and components ([41]).

The EUIPO-Europol *2020 Status Report on IPR Infringement* ([42]) highlights the considerable lack of controls and certification processes during the manufacturing of counterfeit products that leads to the consequent risks to consumer welfare. The spectrum of industries affected by such scant controls covers multiple industries, such as clothing, food, pharmaceutical, electronics, cosmetics, and accessories. These industries carry significant consequences regarding health dangers in connection to substandard (flammable) clothing, dangerous toys, inferior sports shoes or sunglasses. Furthermore, environmental consequences are also in the forefront (e.g. counterfeit pesticides often contain toxic substances that may contaminate soil, water and food).

1.1.4 Liaisons with other criminal activities

The involvement of organised crime groups (OCG) in counterfeiting and piracy is documented by two joint reports by Europol and EUIPO ([43]). The reports highlight the liaisons between IP crimes and other

([40]) https://ec.europa.eu/safety-gate-alerts/screen/webReport.

([41]) EUIPO (2019) *Qualitative study on risks posed by counterfeit to consumers*, June 2019.

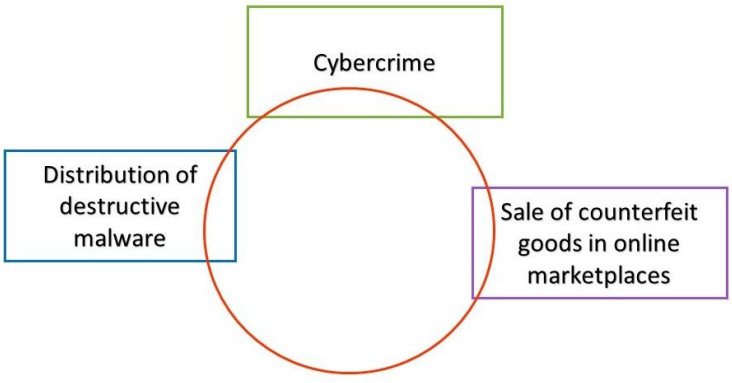
([42]) EUIPO-Europol (2020) *Status Report on IPR Infringement*, June 2020.

([43]) EUIPO-Europol (2019) *Intellectual Property Crime Threat Assessment 2019*, and EUIPO-Europol (2020) *IP crime and its link to other serious crimes. Focus on Poly-Criminality*, June 2020.

other types of crime such as money laundering, food fraud, excise fraud, human trafficking and forced labour. The linkage can occur in two ways, with one criminal activity supporting the other, or as parallel activities carried out by the same OCG. These ways can intertwin in many respect. For example, OCG can produce fraudulent transit documents and use the same route or shipping method for the trafficking of counterfeit goods and other illicit products. They can then use cash-intensive business to launder money generated by the sale of those goods. In turn, these revenues can be used to support other types of serious and organised crime such as drug trafficking ([44]).

Regarding the multiple faces of criminal activity, the cases presented in the Europol-EUIPO reports are indicative of a vicious circle established in the EU territory. This includes EU-based criminal gangs and manufacturers of counterfeit products based in third countries, who organise the importation, transport, storage and distribution of the counterfeit goods within the EU.

In the same spirit, the 2017 *Internet Organised Crime Threat Assessment* (IOCTA) prepared by Europol ([45]) reaffirmed the liaison between digital piracy and more general online criminal activity, and the important threat this liaison poses for our society at large. Cybercrime, distribution of destructive malware, and the sale of counterfeit goods in online marketplaces are strongly intertwined.



Internet Organised Crime Threat Assessment (EUROPOL 2017)

([44]) EUIPO-Europol (2020) *IP crime and its link to other serious crimes. Focus on Poly-Criminality*, June 2020.

([45]) Europol (2017) *Internet Organised Crime Threat Assessment (IOCTA)*.

The sale of counterfeit goods and products via vendor accounts on third party platforms, as well as the application and enforcement of IP rights, both within the EU and globally, are two issues addressed in the *Communication on a balanced IP enforcement system responding to today's societal challenges*, published in November 2017 ([46]). An important aspect of this Communication is its dual goal, that is to say, the improvement of IP enforcement within the EU and the strengthening of customs authorities at the border on one hand, and the initiatives and efforts to confront IP infringement globally on the other. The European Commission takes specific actions to confront online infringement of IP with this Communication, namely the preparation of a 'Watch List' of the most problematic online marketplaces situated outside the EU that are reported to engage in or facilitate IP infringements ([47]).

1.1.5 Emerging trends

Counterfeit and pirated goods are sold online either on stand-alone websites or on third-party platforms. In this study we focus specifically on online sales through third-party platforms. These platforms have made it easier for both businesses and individuals to market any kind of product on a global scale. The misuse of these platforms to advertise, sell and distribute IP-infringing goods 'has become an important source of income for criminal groups engaged in the sale of counterfeit and pirated goods' ([48]).

While the sale of counterfeit goods on online marketplaces is not new, there are some emerging trends that have important implications for IP enforcement.

1.1.5.1 Multiple vendor accounts

Vendors of IP-infringing goods may be 'occasional' or 'systematic' offenders, the latter being part of a larger network of organised crime. Vendors make use of the infrastructure of the online trading platforms

([46]) Communication on a balanced IP enforcement system responding to today's societal challenges https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-707-F1-EN-MAIN-PART-1.PDF.

([47]) Commission staff working document: Counterfeit and Piracy Watch List, Brussels 14.12.2020 SWD(2020) 360 final, p. 35-41.

([48]) EUIPO-Europol (2019) *Intellectual Property Crime Threat Assessment*, p. 11.

to take orders, process payments and communicate with customers (providing shipment details, guiding customers throughout the payment process, etc.). While most platforms have measures in place to verify the identity of the vendor, accounts may be opened under different names for several product ranges whilst operated by the same organisation. These accounts can be subject to take-down requests under the policies of online trading platforms, but the organisation may continue to operate under a different account or network of vendors.

1.1.5.2 Online advertising

Vendors of IP-infringing goods can manipulate and exploit online advertising services by associating their illicit activity with brands. Infringers can buy and place ads on legitimate websites or social media platforms, to direct traffic to external websites selling IP-infringing goods. Typically, these ads target customers with offers of high discounts on branded products. For example, a vendor of counterfeit trainers can falsely advertise a branded shoe on recognised retail sites, diverting traffic from legitimate sales to an illicit, and possibly cheaper, version ([49]).

In 2017, EUIPO commissioned a report examining the extent and structure of digital advertising on websites suspected of infringing IP rights. The study concluded that there was a diversity of advertising on suspected IP-infringing websites, and that 46 % of advertising found on the suspected IP-infringing websites was mainstream in nature ([50]).

([49]) See appendix, case 8.

([50]) See appendix, case 8. More than 1 400 web pages and 180 000 adverts from 280 suspected infringing websites were analysed. The advertisement online ecosystem functions in such a way that makes it susceptive to legitimate products to be advertised, possibly as a result of the '…complex structure of the online advertisement market and the performance incentives of its brokers and agents wishing to maximise the use of adverts across the online advertisement ecosystem...' (Id.). See also EUIPO (2017) *Research on Online Business Models Infringing Intellectual Property Rights – Phase 2, Suspected trade mark infringing e-shops utilising previously used domain names,* October 2017.

1.1.5.3 Social media presence

Social media plays an increasingly important role in the strategies adopted by vendors of IP-infringing goods. Vendors can misuse multiple functionalities that social media platforms offer, to reach a high number of consumers. For example, they can advertise counterfeit goods through posts and messages via public, private or selected group communication, and then direct customers to illegal websites using specific URLs. In addition, social media platforms have developed their own e-commerce facilities or marketplaces, which can be misused to offer IP-infringing goods ([51]).

The integration of social media facilities with online marketplaces, both across platforms and within the same platform, presents new challenges for IP enforcement online. In June 2019, a large operation run by Europol and the Italian Guardia di Finanza, with the cooperation of law enforcement agencies from 13 other countries, led to the closure of over 16 400 social media accounts and 3 400 websites, belonging to two organised criminal groups. The vendors were selling 'a large variety of counterfeit items including clothes and accessories, sports equipment, illegal IPTV set-top boxes, medicines, spare car parts, mobile phones, miscellaneous electronic devices and components, perfumes and cosmetics' ([52]).

A further challenge associated with social media is the use of live-streaming sales with 'influencers' to reach, in particular, young customers. It has been reported that videos promoting counterfeit goods on popular social media platforms can receive tens of millions of views: '… a 20-year-old influencer with over 60 000 followers – has less than 10 000 views on most videos, except those that promote 'dupe' items. Those videos often attract more than 100 000 views …' ([53]). In these kinds of videos,

([51]) EUIPO (2021) *Monitoring and analysing social media in relation to IP infringement*; EUIPO (2021) *Social Media – Discussion Paper. New and existing trends in using social media for IP infringement activities and good practices to address them*, June 2021; EUIPO-Europol (2019) *Intellectual Property Crime Threat Assessment*, p. 37.

([52]) Europol Press Release 'Counterfeit crackdown hits two organized criminal groups with more than 30 suspects arrested', 13 June 2019 https://www.europol.europa.eu/newsroom.

([53]) 'Dupe culture grows on TikTok; why this helps counterfeiters and harms brands'', Tim Lince, World Trademark Review, November 2020.

many counterfeit clothing and footwear products, offered at the lowest prices, are advertised. These offers encompass some of the most famous brands of the fashion industry ([54]).

The phenomenon of 'dupe' counterfeit goods and products is mainly based on the popularity of these products with young audiences. On the social network platforms that target younger consumers, online users are looking for 'influencers' who promote fake goods. The more online consumers follow these 'influencers', the more successful is the business of the producers of counterfeit goods. According to the review, a crucial factor in the combat against 'dupe' counterfeit products would be the increase of consumer awareness regarding the potential dangers and low quality of such products.

1.2 BUSINESS MODEL ANALYSIS

In Phase 1 of the *Research on Online Business Models Infringing Intellectual Property Rights*, commissioned by the EUIPO in 2016 ([55]), an analysis was made on the general structure of business models for online IP infringement. More specifically, the study found that, irrespective of the concrete online business model and its revenue sources, there was a high level of dependence of the operators of IPR-infringing businesses on users and customers who visit their websites or notice their listings on online marketplaces. Therefore, the application by these operators of generally available online businesses tools, such as search engine optimisation, marketing and advertising on social media platforms, is a common phenomenon. Many of the vendors engaged in IPR-infringing activities have also designed apparently well-functioning user interfaces, and '… some vendors even appear to offer the same customer services and use the same customer incentives as legitimate businesses, such as return policies and discounts …' ([56]).

([54]) 'Dupe culture grows on TikTok; why this helps counterfeiters and harms brands', Tim Lince, World Trademark Review, November 2020. See also case 5 in appendix.

([55]) EUIPO (2016) *Research on Online Business Models Infringing Intellectual Property Rights – Phase 1 Establishing an overview of online business models infringing intellectual property*, July 2016.

([56]) EUIPO (2016) *Research on Online Business Models Infringing Intellectual Property Rights – Phase 1 Establishing an overview of online business models infringing intellectual property*, July 2016). The phenomenon has been observed and analysed particularly in relation to IPTV piracy: see EUIPO (2019) *Research on Online Business Models Infringing Intellectual Property Rights – Phase 3 Illegal IPTV in the European Union,* November 2019.

Most of the business models analysed in the 2016 report were operated via an internet site controlled by the infringer, which means that the infringing entity is the registrant of the domain name and that the content on the website is made available by the infringer ([57]). However, operators behind the IPR-infringing activities often either conceal their identities by using privacy shield services for the registration of their domain names, or provide inadequate, false or otherwise misleading contact details on the website, thereby hampering, or even precluding, enforcement actions.

Based on the previous research on online business models infringing IP rights, this section analyses the key elements of the business models used to sell IP-infringing goods through vendor accounts on online trading platforms, starting with the legal definition and classification of infringing goods ([58]).

1.2.1 Infringing goods

IP infringements committed through vendor accounts on third-party trading platforms consist primarily in the sale of counterfeit or pirated goods. However, in order to give a full account of the business models involved, other IP infringements will be included in the analysis. These include the sale of products that are confusingly similar on various grounds to those of legitimate IP owners, or that cause

([57]) EUIPO (2017) *Research on Online Business Models Infringing Intellectual Property Rights – Phase 2, Suspected trade mark infringing e-shops utilising previously used domain names,* October 2017.

([58]) A selection of business model case studies is available in the appendix.

harm to a trade mark's reputation. The analysis also extends to the sale of grey-market products, namely authentic products that are imported and sold without the authorisation of the IP owner.

Figure 2 – Overview of IP infringements

IP infringing goods are defined in various legal instruments and national legislations. These definitions may vary significantly. For the purposes of the present study, a description based on the three broad categories in Figure 2 is used. The aim is to provide a correct representation of the IP infringing goods potentially available on online marketplaces.

From a legal perspective, the sale of counterfeit and pirated goods represents the most blatant form of infringement and, in many cases, the most visible and easily identifiable. In contrast, confusion and brand exploitation encompass both simple and very complex cases, which may require ad hoc examination ([59]). Grey market goods are the most difficult to identify since they are not different from legally imported goods.

([59]) 'Impact Assessment' accompanying the *Proposal for a Regulation of the European Parliament and of the Council concerning customs enforcement of intellectual property rights*, European Commission, SEC(2011) 597 final, p. 29-30.

The key EU legislative instruments to tackle IP infringements are the Enforcement Directive (2004/48/EC) and the Customs Enforcement Regulation (608/2013). This latter leaves grey market goods outside of its scope, and some of its provisions apply specifically to counterfeit and pirated goods to the exclusion of other IP-infringing goods ([60]).

1.2.1.1 Counterfeit goods: fakes and replicas

Although there is no consensus among legal scholars and legislators as to the exact scope of the concepts of 'counterfeit' and 'piracy', it is usually acknowledged that the first denotes goods that infringe trade marks and the latter is generally applied to goods produced by infringing copyright and related rights ([61]).

The Customs Enforcement Regulation (608/2013) provides some guidance in the legal interpretation of those concepts. Article 2(5) defines 'counterfeit goods' as goods bearing a sign that is **either** 'identical' to a trade mark that is registered for the same type of goods, **or** it 'cannot be distinguished in its essential aspects' from such a trade mark ([62]). This definition also encompasses goods infringing geographical indications ([63]) and extends to 'any packaging, label, sticker, brochure, operating instructions, warranty document or other similar item' that bear such identical or essentially identical signs ([64]).

While the concept of 'identical or which cannot be distinguished in its essential aspects' is meant to cover only blatant forms of trade mark or geographical indication infringements, it does not necessarily require that a counterfeit product bears a sign which is an exact reproduction, in all its components,

([60]) *Regulation (EU) No 608/2013 Concerning Customs Enforcement of Intellectual Property Rights*, Olivier Vrins (Kluwer Law International, 2018).

([61]) TRIPs Agreement, Article 61.

([62]) Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003, Article 2(5)(a).

([63]) Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003, Article 2(5)(b).

([64]) Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003, Article 2(5)(c).

to a protected trade mark ([65]). For instance, when goods or services are identical, even a sign that juxtaposes a registered trade mark with other spurious elements can be considered as 'non distinguishable in its essential aspects', provided the protected trade mark retains an independent distinctive role ([66]).

Infringing products falling within the umbrella definition of counterfeit goods can be either 'fake products' or 'replica products':

- **'Fakes'** are counterfeit goods that closely imitate, but are not identical to, products marketed by the brand owner. A broad range of physical products fall into this category. They may be imitations of products bearing a brand, but sold under either another brand or no brand at all. Alternatively, they may be products related, but not identical, to those of the brand owner and sold under its trade mark and logos. An example of the latter are bags bearing a famous brand but having no similarity with any actual bag marketed by the brand owner. Fakes are usually cheaper, substandard quality and are presented to the consumer as non-original products. They fall squarely within the definition of 'counterfeit goods' and are relatively easy to identify.

- **'Replicas'** are counterfeit goods that are closer to the appearance of branded products. Unlike fakes, replicas are intended to deceive, and appear genuine. They are more difficult to identify, and consumers may be misled into believing they are buying an authentic product.

1.2.1.2 Pirated goods

The Customs Enforcement Regulation defines 'pirated goods' more generally as goods resulting from an infringement of copyright and related rights, or design rights ([67]). Copyright-infringing goods include

([65]) *Regulation (EU) No 608/2013 Concerning Customs Enforcement of Intellectual Property Rights*, Olivier Vrins (Kluwer Law International, 2018), § 275.

([66]) *Regulation (EU) No 608/2013 Concerning Customs Enforcement of Intellectual Property Rights*, Olivier Vrins, (Kluwer Law International, 2018), 27/09/2007, C-208/06 and C-209/06, Canon Deutschland GmbH v Hauptzollant Krefeld, EU:C:2007:553.

([67]) Regulation (EU) No 608/2013, Article 2(6).

not only unauthorised copies of copyright works or design articles, but also devices to circumvent technological protection measures (such as mod-chips and game-copiers) ([68]), as well as devices to give access to protected broadcasts (decoder smartcards) ([69]) or to enable illegal IPTV (set-top-boxes and sticks) ([70]).

Examples of design-infringing goods are replica furniture, lighting, rugs, accessories and other design objects.

A particular category of pirated goods is that of illegal software licenses. Unlike other copyrighted digital content, software is subject to the rule of exhaustion of the distribution right after the first sale, and the resale of second-hand software is a legitimate form of trade ([71]). However, the CJEU has also clarified that the rule of exhaustion does not apply to back-up copies of computer programs ([72]). This means that, unlike 'used' software licenses, back-up copies that are offered for sale to third parties should be considered fully-fledged pirated products.

Other examples of pirated digital goods include activation keys for software and video games, and hacked access accounts to online streaming services or databases. The market for these goods or services has progressively superseded the sale of illegal copies of copyrighted content on physical support (CD, DVD, etc.). Finally, an emerging area of digital piracy is the sale of Computer Aided-Design (CAD) files to enable 3D printing of objects protected by design rights or other IP rights ([73]).

([68]) Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Article 6.

([69]) Directive 98/84/EC on the legal protection of services based on, or consisting of, conditional access, Article 2(e).

([70]) Stichting Brein v Jack Frederik Wullems (Filmspeler) (26/4/2017, C-527/15, ECLI:EU:C:2017:300).

([71]) The concept of "sale" for the purpose of exhaustion includes licence agreements (UsedSoft GmbH v Oracle International, 3/7/2012, C-128/11, ECLI:EU:C:2012:407, § 48-49).

([72]) Ranks and Vasiļevičs v Microsoft (12/10/2016, C-166/15, EU:C:2016:762, § 43). Also, section 2.2.1 for a discussion of this case. The business model is presented in the appendix as case 11.

([73]) The Intellectual Property Implications of the Development of Industrial 3D Printing, Dinusha Mendis et al. European Commission (2020).

1.2.1.3 Confusingly similar goods

Confusion occurs when a brand name, logo, colours, packaging and/or advertising themes are used on a related product in a way that tricks or confuses the consumer. This confusion can be achieved in a number of ways, such as by using a similar name or logo on products that are the same or similar to those of the trade mark owner. Under EU law, trade mark infringement occurs when the use in question causes a 'likelihood of confusion', including a 'likelihood of association', between the sign and the registered trade mark ([74]).

Apart from causing confusion in relation to the sign or logo, a product may mislead consumers by using similar packaging colours and shapes. While this may not amount to trade mark infringement, some of the techniques used by vendors to cause customer confusion may amount to unfair competition under national laws or, potentially, a 'misleading commercial practice' under Article 6(2) of the Unfair Commercial Practice Directive. This is defined as practice that, in a certain factual context, 'causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise', and it includes, inter alia, 'any marketing of a product […] which creates confusion with any products, trade marks, trade names or other distinguishing marks of a competitor' and 'any marketing of a good, in one Member State, as being identical to a good marketed in other Member States, while that good has significantly different composition or characteristics, unless justified by legitimate and objective factors' ([75]). Rightsholders may seek civil remedies under the laws of EU Member States on unfair competition.

1.2.1.4 Brand exploitation

This category comprises the unauthorised use of brands on products that have little or no relation to those of the trade mark owner. Typically, famous and instantly-recognisable brand names and/or logos

([74]) Regulation (EU) No 2017/1001 of the European Parliament and of the Council on the European Union trade mark (codification), Article 9(2)(b).

([75]) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (*Unfair Commercial Practices Directive*), OJ L 149 11.6.2005, p. 22. The application od Article 6(2) to the sale of confusingly similar goods has yet to be confirmed by case law.

are placed on goods that are unrelated to those produced by the brand owner. Common examples are the use of luxury brands on mobile phone cases or accessories. However, brand exploitation may take many forms and is not limited to physical goods. An interesting case is provided by the emerging ecosystem of so-called Non-Fungible Tokens (NTF). These are digital objects such as a drawing or an animation, with a unique certificate of authenticity created by blockchain technology. They are sold online in specialised marketplaces as art, using cryptocurrencies, and can reach exorbitant prices ([76]). The sale of an NTF bearing a famous luxury brand is described in appendix A, case 2.

Products falling within this category are IP infringing to the extent that a) the trade mark has a reputation in the EU, and b) the use of the sign takes unfair advantage of, or is detrimental to, the distinctive character or repute of the trade mark ([77]) A case-by-case determination is required to assess whether these conditions are met.

1.2.1.5 Grey-market goods

This category includes authentic goods that are marketed without the permission of the intellectual property owner, such as branded products imported from outside the European Economic Area (so-called 'parallel imports') ([78]) or other authentic goods produced and/or marketed by an authorised licensee in violation of the terms of the licence. Not all of these goods constitute trade mark infringement. When the licence violation concerns only quantitative aspects, as in the case of goods manufactured in excess of the quantities agreed with the IP owner (so-called 'overruns'), the goods are not trade mark infringing, but may be subject to contractual sanctions ([79]). However, trade mark infringement may arise when the goods are produced in violation of qualitative aspects of the licence, as is for instance the case with goods produced by an authorised manufacturer but then rejected by the IP owner because of their poor quality (so-called 'rejects').

([76]) 'Non-fungible tokens are revolutionising the art world – and art theft', *The Guardian*, 12 March 2021. 'Niftygateway' is an example of marketplace offering NFTs for sale: https://niftygateway.com/. Case 2 in appendix.

([77]) Regulation (EU) No 2017/1001 on the EU Trade Mark, Article 9(2)(c).

([78]) 'Trademark Exhaustion And The Internet Of Resold Things', Yvette Joy Liebesman and Benjamin Wilson, in: *Research Handbook On Intellectual Property Exhaustion And Parallel Imports*, Irene Calboli and Ed Lee (Eds.), (Elgar, 2016).

([79]) *European Trade Mark Law*, Annette Kur and Martin Senftleben (Oxford University Press, 2017), 7.47.

Grey-market goods are excluded from the scope of application of Regulation No 608/2013, and they may not be subject to custom enforcement measures ([80]). They are typically presented to the consumer as lawful transactions.

The table below summarises the examples of physical and digital goods in the five categories of infringing goods as defined for the purpose of this study.

	INFRINGING GOODS: EXAMPLES	
	Physical	Digital
Counterfeit	• Fakes (low-quality imitations) • Replica (exact-copy counterfeits)	• Computer Aided-Design (CAD) files for 3D printing.
Piracy	• Copies of copyright content on physical support (CD, DVD) • Replica design objects • TPM circumvention devices • TV decoder smartcards • Fully-loaded set-top-boxes or sticks	• Software copies • Activation keys for software, video games or databases • Hacked accounts for streaming services • Computer Aided-Design (CAD) Files
Confusion	• Look-alike brand name, logo or packaging on similar goods	• Look-alike brand name and/or logo on similar digital goods, e.g. software, video games or apps
Brand exploitation	• Use of famous brands on unrelated goods	• Use of famous brands in virtual worlds or on Non-Fungible Tokens
Grey market	• Parallel imports • Overruns • Rejects	n.a.

([80]) Regulation (EU) No 608/2013, Article 1(5). See *Regulation (EU) No 608/2013 Concerning Customs Enforcement of Intellectual Property Rights*, Olivier Vrins (Kluwer Law International, 2018), par. 119-120.

1.2.2 Online marketplaces

This report focuses on the enforcement of intellectual property rights vis-à-vis the sale of counterfeit and pirated goods, and products involving other forms of IP infringement, through online marketplaces. These are broadly defined as sales platforms where goods (physical or digital) are provided by multiple third parties, and include Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Consumer (C2C) and auction websites. At the time of writing, it is estimated that there are over 50 major online marketplaces available from EU Member states, with the leading presence being that of the global players Amazon (with dedicated and localised websites in France, Germany, Italy, the Netherlands, Spain and Sweden), eBay (with individual sites in most EU countries), AliExpress and Rakuten. Alongside these tech giants are a number of large and very large platforms with a presence extending across various EU countries or with a leading country-specific presence. There are also platforms specialising in certain categories of products (e.g. fashion, food, technology), in second-hand goods, or on specific types of sales (e.g. handicraft products or small brands). In the same vein, some marketplaces specialise in digital goods (e.g. videogames and software licences) or services. Finally, an increasingly important role is played by 'social commerce', namely C2C and B2C sales through social media platforms. Platforms that have developed e-commerce functionalities include Facebook Marketplace, Instagram Shopping and, more recently, TikTok ([81]).

Apart from their size and market share in the EU, online marketplaces are differentiated in terms of types, origin and conditions of products sold, as well as the type of vendors hosted, and customer profiles. In addition, marketplaces differ in terms of vendor registration (on-boarding) and the processes in place to report IP infringements. The available enforcement actions depend largely on which / what kind of marketplace is being used, for what type of infringing activity and by which kind of vendor.

It is crucial to note that the sale of IP-infringing goods on these online marketplaces, is not only an infringement of the rights holder's IP rights, but also a violation of the contractual terms and conditions of the marketplaces, which explicitly forbid activities that infringe third parties' rights ([82]). Moreover,

([81]) 'TikTok takes on Facebook with US ecommerce push', *Financial Times*, 7 February 2021.

([82]) For example, *Intellectual Property Rights Protection Handbook*, Alibaba Group, September 2019, available at https://ipp.alibabagroup.com/.

marketplaces implement deterrent policies against repeat infringers, whereby vendors of counterfeit goods may be permanently suspended from the service ([83]).

1.2.2.1 Wholesale comprehensive marketplaces

These marketplaces contain a large number of categories and range of products. In most cases, the marketplace offers a range of services to vendors, including advertising, marketing and other customer engagement tools, as well as payment solutions, storage and shipping. Marketplaces must comply with regulations to prevent misuse of their services, for example with anti-money laundering laws in relation to payment services ([84]). Instead of storage facilities, some marketplaces adopt a 'dropshipping' model, whereby the seller does not keep products in stock, but purchases items from a third party and ships them directly to the customer. As a result, vendors do not have to handle the product directly, and in most instances they would simply select it from another website.

On-boarding these marketplaces normally entails strict registration and identification processes. Operating the shops, and conducting business through them, requires some degree of expertise in business and e-sales. The IP-infringing goods that are potentially introduced in these marketplaces may be considered the result of systematic and 'professional' counterfeit-selling activities.

1.2.2.2 Marketplaces for auctions and second-hand goods

Like wholesale marketplaces, auction platforms cover a broad range of products and offer additional services like payment and marketing solutions. They are used both for C2C transactions (second-hand goods) and B2C transactions. In this respect, one of the challenges with auction marketplaces is to understand whether a product is an infringing one or a legitimate second-hand product. Some auction marketplaces act as intermediaries for the shipping and require the vendor to post the goods for authenticity checks. This service is optionally available, and only on limited items on the

([83]) *Memorandum Of Understanding On The Sale Of Counterfeit Goods On The Internet*, Brussels, 21 June 2016, section 6.
([84]) *Understanding Financial Crime Risks in E-Commerce*, Anton Moiseienko, RUSI Occasional Paper, January 2020.

marketplace, which marks the respective listing with an ‘Authenticity’ icon. These marketplaces may be misused by both systematic and occasional IP infringers.

1.2.2.3 Marketplaces for independent retailers, and handicraft and art products

These are marketplaces that specifically target owners of non-mainstream brands, as well as independent retailers, free-lance creators (e.g. artists, craftsmen, designers and fashion designers) and hobby enthusiasts. They provide an opportunity for individuals and small businesses to reach a wide global audience and sell their own handmade products or ‘fringe’ products, such as vintage clothing, bags and accessories. The vendors on these websites may infringe third parties’ rights by offering for sale products that imitate or exploit products protected by copyright, design and trade mark rights, although not necessarily counterfeit or pirated goods.

1.2.2.4 Social media marketplaces and stand-alone websites with social media presence

Social media are widely used to promote products that are offered for sale through other e-commerce platforms or stand-alone websites. However, social media platforms are now integrating specific e-commerce functionalities and are rapidly becoming major players as online marketplaces themselves. In this respect, social media can be misused both to infringe IP rights directly, and to support IP-infringing activities occurring through other channels. For example, vendors of counterfeit goods can use sponsored advertising on social media to target customers with deceitful offers of discounts or low prices on branded products offered for sale on external websites. It is very common to have these individual websites in a collection. For example, the same e-commerce platform may be opened under different names for a variety of products, and possibly be operated by the same organisation. Furthermore, ‘burner accounts’ and ‘scam accounts’ that make use of well-known brands can also be used to generate IP-infringing traffic and to spread information about how to get counterfeit products. A technique used by IP infringers is to share a code on social media, so that when a customer places an order from a certain vendor on a marketplace listing an ‘innocent’ item (such a white t-shirt) and

enters the code, they actually receive a counterfeit product ([85]). A further emerging trend is the use of social media live-streaming facilities to promote counterfeit products. Orders are received either via links and/or codes shared during the streaming or directly from the stream's live-chat.

Social media marketplaces offer additional services, comparable to those provided by other online marketplaces, including payment solutions, storage and shipping services. IP infringers can misuse those marketplaces to market IP-infringing goods, taking payments, communicating with customers, and shipping orders.

1.2.2.5 Marketplaces for labour and services

These marketplaces are generally used for providing freelance work such as elements of graphic design, or software development. These services can be misused indirectly to engage in IP-infringing activities, such as web design, packaging and logo design, circumvention of technical measures of protection on videogame and software, or hacking accounts of popular online streaming services. Note that many hacked account details are also sold on marketplaces operating on the Darknet ([86]).

1.2.2.6 Marketplaces for digital goods

The goods marketed in this category of marketplaces are grouped in two broad classes. In the first class, the digital goods are mainly commercial software for which the vendor provides an illicit license. The main techniques and approaches for selling and reselling software activation keys are:

- selling keys from third countries or countries where licences are cheaper than in the country of the customer;
- keys provided to select entities, e.g. to the press, where they will use one key and sell the rest;
- through agreements with education partners, e.g. university staff and student accounts;

([85]) case 5 in appendix.

([86]) section 1.2.3.

- through volume licensing, where a key can be used from multiple users and/or more than one number of computers.

Users can buy keys to activate downloaded commercial software ([87]).

The second category refers to the emerging marketplaces of blockchain-certified digital art, namely visual images and short animations that can only exist in a digital form, and which are accompanied by proof of ownership guaranteed by blockchain technology. All transactions relating to these digital art objects are recorded using so-called non-fungible tokens (NFT), which are essentially cryptographic tokens that are unique and not mutually interchangeable. Having ownership information on the blockchain makes an illegal sale of a copy virtually impossible.

1.2.3 Darknet marketplaces

Darknet marketplaces include a vast area within the internet ecosystem that is dedicated to illegal conduct, sales and services taking place below the surface of the 'visible' internet **([88])**. Darknet marketplaces facilitate transactions of a wide range of counterfeit products, normally by means of cryptocurrencies. In July 2017, two of the largest darknet marketplaces (AlphaBay and Hansa) were taken down during an international operation led by the US Federal Bureau of Investigations (FBI) and the Dutch police, with the support of Europol. As reported by Europol:

> Prior to its takedown, AlphaBay, the largest market, reached over 200 000 users and 40 000 vendors. There were over 250 000 listings for illegal drugs and toxic chemicals, and over 100 000 listings for stolen and fraudulent identification documents (IDs), counterfeit goods, malware and other computer hacking tools, firearms, and fraudulent services. Since its creation in 2014, transactions concluded in the market were estimated

([87]) cases 12 and 13 in appendix.

([88]) *Inside The Deep & The Dark Web,* Cyber Security Intelligence, News Analysis, published 22 June 2020, available at https://www.cybersecurityintelligence.com. For a further analysis on enforcement strategies in the Darknet see section 2.1.3.

to have netted USD 1 billion. Hansa was the third largest criminal marketplace on the Darknet, trading similarly high volumes of illicit drugs and other commodities ([89]).

In January 2021, DarkMarket, allegedly the world's largest darknet marketplace, was taken down in an international operation led by Germany with the support of Europol ([90]).

In spite of the governments' enforcement actions, darknet marketplaces adapt very quickly to shutdowns and adopt new ways to circumvent restrictions. Products of luxury brands from the clothing, accessories, footwear, and cosmetics industry are to be found in these marketplaces, where there can be discounts of up to 90 % of the authentic product's price ([91]). From a technical point of view, all the consumers have to do is to download the encrypted browser Tor, which allows access to anonymous black-market vendors.

Most Dark Web marketplaces attempt to moderate and arbitrate the transaction between the vendor and the buyer, through the use of escrow accounts. For example, a vendor on a Darknet marketplace sold over 200 items advertised as a 'high-end replica' of a famous brand's t-shirt. The vendor used IP address anonymisation (The Onion Routing protocol) to hide the location of the marketplace and shipped the items from Hong Kong ([92]).

1.2.4 Marketplace types and categories of infringing goods

The sale of IP-infringing goods can be differentiated by the following broad features:

- marketplace type (see descriptions in sections 1.2.2 and 1.2.3);

([89]) *Intellectual Property Crime on the Darknet*, Europol, 2017, https://www.europol.europa.eu/publications-documents/

([90]) *DarkMarket: world's largest illegal dark web marketplace taken down*, Europol Press Release, 21 January 2021. https://www.europol.europa.eu/newsroom.

([91]) *The Darknet Counterfeit Gift Guide: Chanel, Rolex and Louis Vuitton,* Molly Fitzpatrick with Gordon Bottomley, 22 December, 2014, available at https://www.vocativ.com.

([92]) Case 9 in appendix.

- category of infringing goods (counterfeit, piracy, confusion, exploitation and grey market – see section 5.1);
- whether the seller is hiding or declaring the fact that their product is non authentic (e.g. if they are attempting to trick the customer into believing that they are buying a genuine product at a discounted or low price).

The five categories of IP-infringing goods are not uniformly distributed in the different marketplaces. The following figure is indicative of the likelihood of detecting a particular kind of infringing good in each type of marketplace.

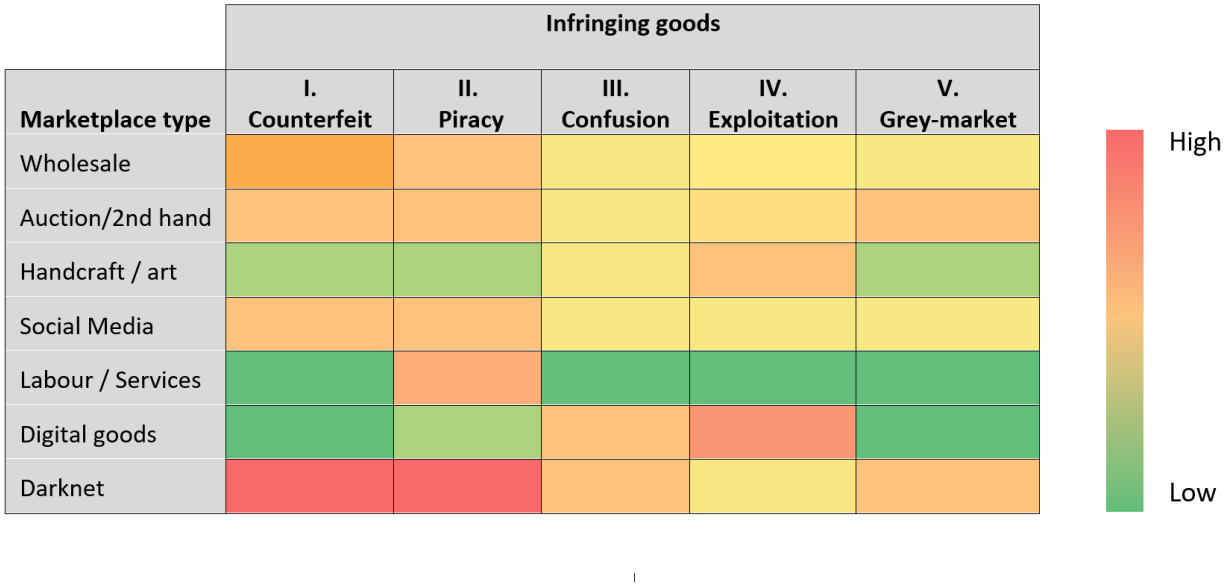


Figure 3 – Marketplace types against categories of infringing goods

1.3 THE IP INFRINGEMENT SUPPLY CHAIN

1.3.1 Introduction

This section presents a view of the supply chain for the process underlying IP infringement via vendor accounts on third-party trading platforms. In accordance with most supply chain approaches, the different stages of the chain should be read as part of a continuous process from the supply of raw material for the production of the counterfeit product to the delivery of the product to the end consumer, through a flow of information, physical items and money that involves a number of intermediaries.

There are seven stages identified in the supply chain. From an enforcement perspective, it can be expected that the visibility is reduced as we traverse back the supply chain (right to left) and is increased as we approach the customer (shipping, far right).

Figure 4 – The Counterfeit supply chain

Every activity in the chain is represented with an **action card** placed into one or more of the echelons accordingly. These action cards illustrate the activities relevant to each specific stage of the supply chain – both for the **infringers** and for the **investigators or preventers**. The activities can be conducted in the physical world, cyberspace, or both. However, an activity may be performed exclusively by either an infringer or a law (or self-regulatory) enforcement entity. For every infringing activity, we attempt to describe a matching investigative or law enforcement action.

- On the infringer's side, the supply chain illustrates the **activities** that are required to produce, store, distribute, promote, sell and ship the counterfeited product, along with the techniques that are used to elude enforcement actions, for example techniques to evade detection, take-down, confiscation or seizure of goods.

- On the investigator's or preventer's side, the scheme illustrates the actions that can be taken by **enforcement actors** at each stage of the chain. These actions include investigation, law enforcement, and self-regulatory measures of enforcement.

The seven stages are depicted in the high-level supply chain diagram in Figure 4.

The following observations and points accompany the counterfeit supply chain.

- The stages of the chain do not always follow the prescribed order (i.e., the shipping process can occur between other stages too, especially in the cases where there is an established network or customer base).

- Occasionally, some of the stages may be omitted (or may not be possible) during an enforcement action, as visibility is expected to drop as the chain is traversed from right to left.

- The geo-socio-political aspects may affect the effectiveness and delivery of an investigation and associated actions. For example, attempting to take down and interfere with the production in a particular country may trigger events with the local society and authorities (e.g. the take-down of a production factory that employs thousands of workers in a third world country).

- Investigating some stages might be of less value in some use cases but can be considered critical in cases where human life and safety is under threat (e.g. when investigating the raw material supply for the production of counterfeit pharmaceutical products).

In the following series of tables, the corresponding activities for the respective stages are described. The labels describe the kind of activity involved at each stage of the chain.

Physical: this label means that the activity is conducted by means of physical interactions.

Cyber: the activity occurs on the internet.

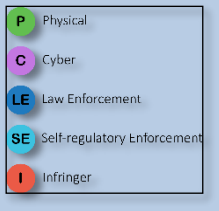
Law Enforcement: the activity is mainly performed by law enforcement agencies.

Self-regulatory Enforcement: the activity is conducted by the rights holders or by third-party companies, such as online marketplaces, payment services or shipment companies.

Infringer: This label shows that the activity is an infringing activity used by the perpetrator.

1.3.2 Raw material supply

1. raw material supply

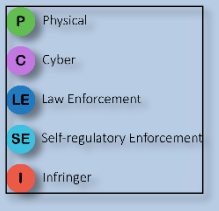


The supply of raw materials can involve the same sources as the original products, or even, in some cases, refer to semi-completed products, where the infringers have managed to tap into the original production line.

Activity	Scope	Description
Supply of potentially dangerous materials (PDM) / uncertified materials	C P I	This is the main activity of the infringer. In some cases (e.g. pharma), there may be health and safety consequences to the consumer/public.
Monitoring of specific materials	C P LE	Identification of hotspots where the materials are produced or originate from has the potential to significantly disrupt the supply chain. Maintaining a database of locations for specific products can be achieve by consolidating information from previous cases, and in cooperation with brand/IP holders (where applicable).
Customs checks	P LE	Leverage of historical information from countries of origin / known hotspots and information on the declaration forms (e.g. Bill of Lading). This activity would be greatly improved by streamlined collaboration between Customs and law enforcement agencies.

1.3.3 Production

2. Production



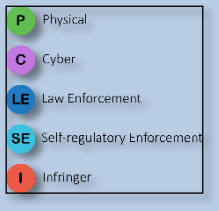
The production of counterfeit products can take place on various occasions and scales; ranging from businesses run by a single person or a small team, to small/medium factories and large factories that employ thousands of people.

Activity	Scope	Description
Facility take-downs	C P I	By closing the facilities that produce the illicit items, law enforcement agencies can interrupt the supply decisively, at its beginning, before the items are distributed to vendors. The process can be considered delicate, and requires cooperation with local authorities.
Block bank accounts	LE	Blocking the producer's bank accounts deprives them of the assets that finance production of the illicit items.
Follow trends	C SE	Seasonal events (e.g. beginning of sporting events, music concerts, release of popular products) affect the production of goods. This is increased for items that are relevant to them.
Production by demand	C P I	The production of illicit products can be based on an agreement between the production facility and a vendor that requires a specific item that may be popular in a specific market (e.g. a specific t-shirt that is popular among the citizens of a country) or during a specific season (e.g. football events).
Continuous production	P I	Some products are constantly produced illicitly, because the demand for them is constant, and the product remains unchanged within time (e.g. a shampoo or a product that fights flu symptoms).

Use of hazardous materials	P I	Often, the producer of the illicit items, for a variety of reasons (e.g. availability of materials, low cost etc.), uses substitutes or material that can be proven hazardous. In these cases, the cost is not only financial, but may also include effects on the consumer's health, safety, or the environment.
Part-by-part production	P I	The production of an item can be done in parts so that the item remains undetected and avoid recognition as an illicit item (e.g. the logo of a shoe is produced by another unit from the rest of the shoe, for assembly near the selling point/stage).

1.3.4 Storage and inventory

3. Storage & Inventory



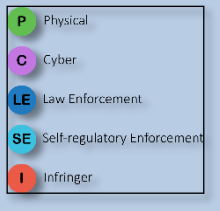
Before the distribution to the market, or even before sending directly to the buyers, the products are stored in locations that may not be the production units. These include fulfilment centres operated by online marketplaces. These locations can differ in size, and belong to the producers, the vendors or even a third party that acts as the relay agent between the two ends.

Activity	Scope	Description
Confiscation/seizure	P LE	Raiding the IP infringers' inventory and seizing the infringing items. This action is accomplished by law enforcement agencies and is considered a physical action.
Bulk storage	P I	The storage of infringing goods ,in a large quantity, in a dedicated depot/spot by the counterfeiters. Depending on the type and nature of the counterfeit

		goods, bulk storage locations may be areas such as industrial zones, etc.
Local storage	P I	The storage of the infringing goods in separate local depots/spots by the counterfeiters. Local storage means that the storage spot is close to where the counterfeit products are being sold and/or being shipped. These may include high-street market shops.

1.3.5 Online offer of sale

4. Online offer of sale



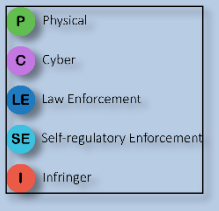
The infringers take advantage of the capabilities offered by the internet to offer the counterfeit products to people, far exceeding their geographical radius. While trying to evade detection, they can either use already existing platforms or rely on other infringing websites and sell the products to their users.

Activity	Scope	Description
Liaison with platforms	C LE SE	Increased communication among the stakeholders can improve the detection and removal of the vendors of the illicit items that are hosted, unknowingly, by the platform.
Take-down procedures	C LE SE	The taking down of websites (in the case of an infringing website) or accounts (in the case of a vendor in a marketplace).
Sale to customer	C I	Vendors of illicit product can also sell directly to the end customer, circumventing marketplaces or other distribution mediums.
Production to retail	C I	The illicit products can be delivered to the retail industry. Owners of retail shops can be found selling counterfeit products – knowingly or in the belief that they are providing original products to their customers.
Production distributed to large marketplaces	C I	Vendors of counterfeit products can take advantage of the infrastructure and popularity offered by a marketplace and offer their items online. Depending on the vendor and the platform, some items can be sold as originals, while others can be sold as imitations, counterfeits, etc.
Production distributed to infringing websites	C I	Illicit vendors can offer their items through websites created specifically for their needs. The sites

		contain all the necessary information for the products, the payment and the delivery method. These sites either sell products by advertising them as original or openly sell them as counterfeit.
Evasion techniques for distribution through large marketplaces	C I	To avoid detection and having their accounts removed, the vendors use a series of evasion techniques that can involve: fake credentials for the registration process; use of images of original products, etc; masking the order by linking the purchase to a decoy product, etc.
Detection evasion techniques for customs controls	C I	In order to avoid detection and having the products confiscated in customs, the vendors use multiple methods to hide the identity of the illicit items. For example, tape with instantly-recognisable logo and name of a major marketplace can be used to wrap items, shipments can contain both original and illicit items, or declare different products.
Infringing websites	C I	Vendors may create and maintain their own website to offer the products. The sites can be unique or there can be multiple different sites (with similar or different names) that have similar or identical structures, contain the same information, and are administrated by the same entity.

1.3.6 Marketing

5. Marketing



The marketing techniques refer to all the methods used by the infringers to make the products known and/or appealing to potential buyers. The items for sale can be advertised as original products or even sold openly as counterfeit, and the perpetrators can use all the possible options offered by technological advancements. Services that can be used to market IP-infringing products include paid advertising and promotion through public social media posts, using specific hashtags to attract users.

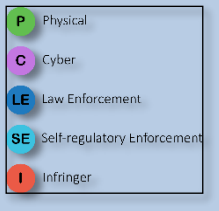
Activity	Scope	Description
Follow flags	C LE SE	There are several indicators that may alert law enforcement with regard to a marketplace or online website, such as offers that are: • 'too good to be true'; • have a substantial discount; • receive an inflated amount of positive feedback in a short time. This is considered a cyber-activity that is conducted by law and self-regulatory enforcement organisations.
Monitor communications	C LE SE	Law and self-regulatory enforcement agencies follow the online communications to identify counterfeiters from public posts or live-streaming broadcasting on social media platforms. Monitoring communication via private networks such as peer-to-peer applications (instant messaging, groups, etc), and advertising applications requires intervention from law enforcement.
Socmint (social media intelligence) for infringing websites	C LE SE	This activity represents a category of cyber-intelligence activities that are conducted on social media platforms.

Listing and advertisement takedowns	C LE SE	This encompasses takedowns of ad keywords, de-listing results on search engines, and removal of a particular product or complete seller account from a marketplace.
Marketplace	C I	Counterfeiters in some cases register on well-known marketplaces to use the marketplace's value to advertise their infringing products.
Infringing websites: advertising activity on messaging platforms	C I	Infringing websites that contain links to messaging platforms chats for receiving orders, and provide information on payment and shipments, are involved in this activity. It is common for infringers to guide the buyer to a payment website with no information/flag on the counterfeit product, to evade detection or legal implications. Therefore, it is important for them to establish one-to-one contact with the buyer through these messaging platforms. Furthermore, these platforms are utilised to establish their customer portfolio.
Infringing websites advertising activity on blogs	C I	Referrals from low-profile blogs to infringing websites are used to advertise the counterfeit products.
Online ads containing infringing material	C I	Marketing through online advertisements.
Darknet marketplaces	C I	Marketing on Darknet marketplaces. The buyers from these marketplaces generally know that they are buying counterfeit and in many cases the sale is wholesale.
Obtain fake identification/stolen credentials from Darknet	C I	Fake credentials are obtained for use selling/distributing/shipping counterfeit products, registering the marketplaces and also to create fake identities for exchanging cryptocurrency to fiat currencies.

Live stream sales	C I	Social media live-streaming facilities are used to market and demonstrate the product to buyers. One interesting characteristic of live-stream sales is that the orders are received via the chat of the live sale. Therefore, once the stream is over, there is no evidence left to trace.
Marketing through influencers	C I	Influencers from major social media platforms are selected and used for marketing and promotion of the goods.

1.3.7 Sales

6. Sales



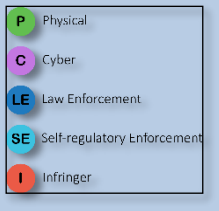
The actual financial transaction for the purchase of a counterfeit product is either a digital transaction or a transaction with a physical monetary exchange. In both cases, a series of steps can be used to mask the activity. Therefore, investigations require 'follow-the-money' procedures and cooperation between law enforcement and financial institutions.

Activity	Scope	Description
Liaison with banks/ financial institutions	LE SE	This will help authorities detect and identify the entities behind the financial transaction, and proceed to the necessary actions required for blocking the right bank accounts.
Liaison with payment service providers	LE SE	This liaison can protect the customers by allowing a refund for unknowingly purchasing fake products or even blocking the transaction, when it comes to identified illicit vendors.
Follow-the-money investigations	LE	'Follow-the-money' investigations are the outcome of the aforementioned liaison activities. The authorities, once they collect all the necessary evidence, can create a full profile of the vendors by analysing the financial transactions under investigation.
Test purchases	C P LE SE	Purchasing a fake product offers the authorities the evidence required to build a case against an illicit vendor. Usually, two test purchases are required when an investigation reaches a courtroom.
Cryptocurrency payment	C I	Darknet purchases can be accomplished with the use of cryptocurrency, which offers the anonymity that is required from illicit actors. This is also applicable in cases of infringing websites.

Online payment – digital wallet service	C I	'Digital wallet' is an alternative method of online payment that can also provide anonymity. It can be used to avoid online payment service providers and to set up quick payments by the illicit vendors.
Online payment – credit card	C I	The use of credit card transactions as the established method of payment for online transactions. With the appropriate liaison with banking institutions and payment service providers, these transactions are easier to follow than other payment methods.
Cash payment – mules	P I	Where a cash payment is feasible, a third person can be used to deliver the payment from the buyer to the seller.
Cash payment – in store purchase	P I	Fake products can also be sold in physical stores. In this case, cash payment is easier and can easily be masked.
Cash payment – from seller	P I	Vendors of illicit items can pay the producers in cash, either by using a money mule, or directly. The process can be hidden and remain undetected, rendering the 'follow-the-money' process challenging.
Pay by postal order	C P I	Payment with postal orders can also remain undetected and attract minimum attention. No bank accounts or other financial details are required for such payments.

1.3.8 Shipping

7. Shipping



Once the financial transaction is executed, the product is shipped to its new owner. The owner can either be the end-buyer or an entity that will distribute the product on the market. The products are delivered globally with the use of usual cargo procedures. The shipments differ in size and quantity.

Activity	Scope	Description
Liaison with courier/post services	P, LE	Law and self-regulatory enforcement agencies can liaise with courier and post services to prevent distribution of counterfeit products and/or identify the address of the vendor through the postal addresses that the infringers use.
Liaison with Customs	P, LE	Law and self-regulatory enforcement agencies can liaise with customs to prevent distribution of counterfeit products and/or identify the addresses through the postal addresses that the infringers use.
Monitor routes	C, P, LE	Routes of transfers are identified in this activity to discover the origin of the product, the individual distributers and vendors, and how the products are handed over from (underground) factories to the buyers.
Monitor suspects	C, P, LE	Monitoring routes of shipment leads to monitoring those suspects that receive unusual amounts of unexpected orders from regular routes. Monitoring suspects and their shipment activities might also lead to the identification of new routes and shipment methods.
Seizure of goods	P, LE	Seizure of goods at the customs or postal services can be conducted by border forces.

Shipping in bulk amounts	P I	Infringers may ship products to distributers and vendors in one-off bulk amounts.
Shipping in limited amounts	P I	Infringers may ship products in small amounts to evade being detected at customs.
Hybrid shipping models	P I	Infringers may ship bulk amounts (containers) of pre-prepared small parcels to be mailed to customers once the container has entered the Foreign Trade Zone.
Changing routes for shipments	P I	Infringers may regularly alter the routes they use to evade being detected.
Shipping mixed with original products	P I	In some cases, original products are sent at the same time to avoid detection and keep a legal profile with the courier services.
Shipping part by part (assembly at destination)	P I	Some products can be sent as parts in an attempt to evade or weaken cases of copyright infringement. An example would be sending logos and products separately; or sending left and right shoes separately.
Dropshipping	P I	This is a retail method where a vendor does not keep the products it sells in stock. Instead, when a vendor sells a product, it purchases the item from a third party and has it shipped directly to the customer. As a result, the seller does not need to handle the product directly ([93]).

([93]) https://www.shopify.com/blog/what-is-dropshipping#definition

2. ENFORCEMENT AGAINST INTELLECTUAL PROPERTY INFRINGEMENTS ON THIRD PARTY TRADING PLATFORMS

2.1 MEASURES, POLICIES AND TACTICS

This section presents a review of the key measures, policies and tactics that are available to tackle IP infringements on online trading platforms. The review starts with an analysis of the voluntary measures adopted as an effect of the ongoing collaboration between rights holders and platforms, and includes examples of good practice aimed at preventing infringing activities by vendors ('proactive measures') as well as at repressing or limiting the effect of those activities once they occur ('reactive measures'). **Furthermore, the review looks at the policies and tactics** adopted by rights holders and law enforcement agencies to investigate IP infringements and enforce IP rights, taking into consideration the actions available at each stage of the supply chain discussed in the previous section.

2.1.1 Proactive measures

A number of proactive measures have been developed by online trading platforms in the framework of voluntary agreements with rights holders. Of paramount importance in the EU is the Memorandum of Understanding (MoU) promoted by the European Commission in 2011 and revised in 2016, which is currently signed by 30 stakeholders, including major rights owners, online platforms and business associations ([94]). The MoU is a voluntary agreement to hinder the sale of counterfeit goods on online marketplaces, based on a principle of differentiated responsibility and standards of 'commercial reasonableness' ([95]).

([94]) European Commission, *Memorandum of understanding on the sale of counterfeit goods on the internet*, https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en.

([95]) Memorandum of Understanding, 21 June 2016, Brussels, p. 2.

On the one hand, rights holders commit to engage themselves in specific and commercially feasible measures such as ([96]):

- effective fighting against counterfeiting at its source, including at points of manufacture and initial distribution;
- active monitoring of offers on the websites of online platforms, to identify counterfeit goods and notify online platforms of their existence;
- supplying online platforms with information that could help identify counterfeit goods, including information on goods that are particularly susceptible to being counterfeited and keywords commonly used by vendors for offering for sale obviously counterfeit goods.

On the other hand, online marketplaces commit themselves to engage in specific commercially and technically feasible measures such as ([97]):

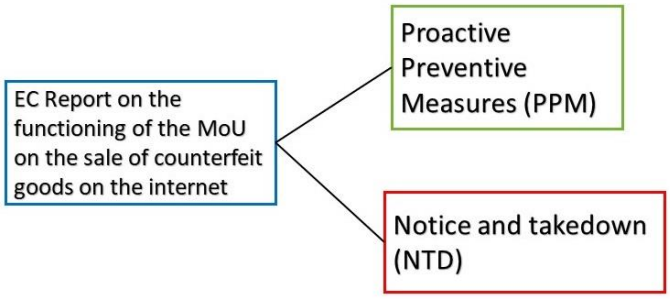
- requesting from the vendor all their contact information and verifying the vendor's identity;
- considering all the information provided by rights holders that could help identify counterfeit goods;
- identifying, and blocking the sale of, counterfeit goods, and blocking the offer of such goods through their online services.

As a result of the MoU, a number of good practices have been developed. These belong to two broad categories, namely a) proactive and preventive measures (PPM), aimed at blocking offers of counterfeit or pirated goods from appearing online in the first place, and b) notice and takedown (NTD) procedures to promptly remove those offers from the marketplace ([98]).

([96]) Memorandum of Understanding, 21 June 2016, Brussels, p. 2.

([97]) Memorandum of Understanding, 21 June 2016, Brussels, p. 2.

([98]) European Commission, Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet, Brussels, 14.8.2020, SWD(2020) 166, final/2.



This section addresses the first prong of these good practices, namely PPM developed by online marketplaces.

2.1.1.1 Contractual obligations deriving from Terms and Conditions (T&C)

Registering a vendor account on an online marketplace implies acceptance of Terms & Conditions (T&C) as well as other policies that may apply to specific services. Typically, T&C prohibit the sale of goods that infringe third parties' IP rights. Therefore, marketplaces can take immediate action against IP-infringing users on the basis of breach of contractual obligations. In particular, they can remove listings, deny access to certain features or functionalities, or suspend or terminate accounts.

T&C may include specific provisions on IP infringement, in particular policies against **repeat offenders**. These policies make clear that users who repeatedly violate the T&C may have their accounts suspended or disabled. However, repeat infringement policies are effective only when coupled with ID verification and traceability systems, in order to prevent suspended or disabled users from returning and signing in with a different account.

2.1.1.2 Identity verification and traceability of traders

Some online marketplaces require users to provide valid identification, such as proof of identity or an address, as a condition for opening a vendor account. In a similar vein, users who intend to register as a corporate entity may be required to provide proof of a business licence or other relevant permits.

These requirements are not easy to implement and can be circumvented in many ways ([99]). However, they may represent a deterrent to users aiming to return after being disabled, or who open multiple accounts. Some social media platforms also allow users to report fake profiles ([100]).

Identity verification requirements include measures to undermine the creation of multiple accounts by a single user. Additionally, marketplaces may also restrict the use of certain keywords in profile names – for example the use of well-known trade marks – and require proof of ownership or legal qualification before activating the profile ([101]).

The principle of trader traceability, also known as the 'know your business customer' (KYBC) requirement, has been formally introduced in Article 22 of the proposed Digital Services Act (DSA) Regulation ([102]). Once in force, this provision will oblige online platforms to receive, store, make reasonable efforts to assess the reliability of, and publish specific information on the traders using their services, where those online platforms allow consumers to conclude distance contracts with those traders.

([99]) See, generally, Stephen Mason 'Trust' between machines? Establishing identity between humans and software code, or whether you know it is a dog, and if so, which dog?, *C.T.L.R.* 2015, 21(5), p. 135-148.

([100]) EUIPO *Monitoring and analysing social media in relation to IP infringement* (2021); EUIPO *Social Media – Discussion Paper. New and existing trends in using social media for IP infringement activities and good practices to address them*, June 2021, p. 29.

([101]) See for example Alibaba Group, *Intellectual Property Rights Protection Handbook*, September 2019.

([102]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 22.

2.1.1.3 Technological measures of prevention and traceability of products

Many marketplace platforms have developed proactive measures to reduce listings for IP-infringing goods ([103]). Examples of the tools available to rights holders on major platforms are ([104]) the following.

- **Alibaba Intellectual Property Protection Platform**, which is meant to 'facilitate rights holders on intellectual property right protection in a cooperative manner over various Websites under the Alibaba Group' ([105]). According to the group, proactive measures, enabled by AI technology, allowed up to 96 % of listings for IP-infringing goods to be detected and removed after posting, before a sale could be made ([106]). The group also claims to have 262 patents 'tied to its core anti-counterfeiting technology' and to contribute to combating counterfeit sales through civil litigations and other actions. In 2020, for the first time, 'blockchain-based evidence-preservation technology […] resulted in evidence recognition and admissibility in court for intellectual property right (IPR) infringement litigation' ([107]).

- **Amazon Brand Registry**, which provides a set of tools, including keyword and image recognition, and Amazon Standard Identification Numbers (ASINs) are used to prevent the sale of infringing products. Proactive services also include 'Transparency', a system where each item is provided with a unique code to verify its authenticity before it reaches the customer, and

([103]) For an overview of technological PPM see Sylvia Polydor 'The interplay between technology and trademark protection: a study of infringement, intermediary responsibility and protection measures in the digital age', *E.I.P.R.* 2020, 42(1), p. 4-12.

([104]) UK Intellectual Property Office *Protecting Intellectual Property Rights on e-commerce stores* https://www.gov.uk/government/publications/protecting-intellectual-property-rights-on-e-commerce-stores/protecting-intellectual-property-rights-on-e-commerce-stores [accessed May 2021].

([105]) https://ipp.alibabagroup.com/policy/en.htm

([106]) Adam Najberg 'Alibaba, Partners Notched Strong IPR Protection Gains in 2020', *Alizila (News from Alibaba)*, 26/03/2021, https://www.alizila.com/alibaba-partners-notched-strong-ipr-protection-gains-in-2020/.

([107]) Adam Najberg 'Alibaba, Partners Notched Strong IPR Protection Gains in 2020', *Alizila (News from Alibaba)*, 26/03/2021. In the 2018 Report, the Alibaba Group claimed to have initiated 83 civil litigation actions and delivered over 1 900 suspects and the closure of more than 1 500 facilities (Alibaba Group (2018) *Global Intellectual Property Rights Protection Annual Report* (May 2019), https://www.alizila.com/wp-content/uploads/2019/05/Final_Alibaba_2018_IPR_Report.pdf).

'ProjectZero', a tool for scanning and automatic removal of suspected counterfeit items based on machine-learning technology ([108]).

- **eBay Verified Rights Owner Program ('VeRO')**, consisting of keyword filtering, content moderation on flagged listings, and restrictions on the sale of selected 'High Risk Brands' ([109]).

- **Facebook Marketplace 'Commerce & Ads IP'**, a tool that allows IP owners to search for their registered trade mark in ads, Shops content, Instagram posts with product tags, Marketplace posts and Facebook group sale posts, and to identify and report infringing content.

Social media and messaging applications also make tools available that let brand owners protect their identities and content on a proactive basis ([110]). For example, Weixin/WeChat has set up a keyword-based interception mechanism to halt the registration of suspect accounts and require proof of 'legal qualification' ([111]).

2.1.2 Reactive measures

Voluntary measures to repress or minimise the impact of IP infringements include 'notice and takedown' procedures and other mechanisms to detect, identify and hinder the availability of infringing goods on online trading platforms.

2.1.2.1 Notice and takedown procedures

The aim of NTD procedures is to streamline the process of notification and removal of infringing content that is made available online. These procedures have been introduced in the EU as an

([108]) https://brandservices.amazon.co.uk/.

([109]) https://www.ebay.co.uk/help/policies/listing-policies/selling-policies/intellectual-property-vero-program. The system is described by Arnold J. in *L'Oreal SA v eBay International AG* [2009] EWHC 1094 (Ch), p. 79-86.

([110]) EUIPO (2021) *Social Media – Discussion Paper*, § 6.1.2.

([111]) *Weixin Report on Protection of Brand Owners*, March 2018.

optional condition for an online intermediary which seeks to take advantage of liability exemptions offered by the e-commerce Directive ([112]). Indeed, Article 14(1)(b) of the e-commerce Directive requires 'Information Society Service Providers' (ISSPs) to act expeditiously to remove, or disable access to, the information upon discovering evidence of illegalities, in order to benefit from the exemption ([113]). NTD systems fit in this context, where notice by rights holders serves as disclosure or information of illegal activities, and expeditious action by ISSPs as a response to this disclosure or information. NTD systems (also known as 'notice-and-action') are a key component of the voluntary measures implemented in the context of the 2016 Memorandum of Understanding, and feature prominently in the Commission's *Recommendation on measures to effectively tackle illegal content online*, published in March 2018 ([114]).

However, it is notable that this procedure is not mandatory under EU law; there is no standardised procedure that Member States are obliged to comply with. This is in contrast with the law in other jurisdictions, such as the US or China, where NTD systems are statutorily detailed ([115]).

Nevertheless, NTD procedures represent the main way that rights owners currently work with online platforms to remove listings for counterfeit and pirated goods. According to the good practices developed in the framework of the MoU, effective NTD procedures (as implemented by most online marketplaces) include the following:

- **a clear information package for rights holders**, with detailed instructions on the information that must be submitted to identify the infringement, as well as the information required as proof of ownership or legal entitlement to enforce an IP right, and thereby activate the notification;

([112]) European Commission, Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet, Brussels, 14.8.2020, SWD(2020) 166, final/2, p. 23. For a thorough discussion of the legal basis of NTD see Knud Wallberg, 'Notice and takedown of counterfeit goods in the Digital Single Market: a balancing of fundamental rights', *Journal of Intellectual Property Law & Practice* (2017), 1.

([113]) See discussion infra, section 2.3.3.

([114]) Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final).

([115]) Graeme Dinwoodie, 'A Comparative Analysis of the Secondary Liability of Online Service Providers' in Graeme Dinwoodie (ed), *Secondary Liability of Internet Service Providers* (Springer 2018) 40.

- **tools to manage multiple notifications**, or 'in-bulk' requests, enabling rights holders to include multiple infringing listings in a single takedown request;

- **'trusted flaggers' programmes**, with fast-track, privileged channels for notifications and more expeditious removal for 'trusted' rights holders with specialised expertise and dedicated technology for the detection and identification of infringing content;

- **search and report tools**, to facilitate the process of searching potentially infringing content on the platform, by means of image recognition and other technologies ([116]);

- **information for users** on the reason for the removal and the potential consequences of repeated infringements, as well as easily accessible information on the right to appeal or **counter-notice procedure** to challenge the notice of the IP owner.

NTD procedures are, in principle, available to owners of any IP right enforceable in the EU, including owners of both EU and national trade marks. Additionally, platforms may allow users to report other vendors' listings suspected of infringing trade marks, as well as other possible policy violations and inappropriate content.

Online marketplaces can exchange information related to NTD procedures with law enforcement authorities, in particular, customs, police and market surveillance authorities ([117]). Additionally, they inform the relevant actors of the reaction that has taken place, as a follow-up to the notice. For example:

- acknowledging receipt of the notice, and informing the notifier of the outcome of the assessment and the proposed next steps;

([116]) See infra, section 2.1.2.2.

([117]) European Commission, Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet, Brussels, 14.8.2020, SWD(2020) 166 final/2, p. 31-36.

- in the case of a justified notice, and a removed offer, informing the vendor and explaining why the offer was removed, who submitted the notice, and what actions they can take to appeal (e.g. filing a counter-notice within a reasonable period; contacting the notifier) ([118]).

Rights holders, for their part, should submit the notices as soon as possible after detecting the IP-infringing offer, provide sufficiently detailed and substantiated notices, and exchange information on the use of dedicated automatic reporting tools to speed up the processing of notifications as a prerequisite for platforms to learn about trends and improve systems (machine learning, training algorithms) ([119]).

2.1.2.2 Automated detection measures

Major online marketplaces have developed technological solutions to detect suspected infringing content by means of artificial intelligence and machine learning. These systems constitute an increasingly important part of the programmes developed in collaboration with rights holders, which have been already addressed in the context of voluntary proactive measures ([120]).

Search tools made available to rights holders to identify infringing content involve the analysis of a wide range of 'signals', including, most notably: combinations of brand names and keywords in the title and text of the listing; price charged for a certain product; detection of brand name or logo via image recognition.

([118]) European Commission, Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet, Brussels, 14.8.2020, SWD(2020) 166 final/2, p. 26-27.

([119]) European Commission, Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet, Brussels, 14.8.2020, SWD(2020) 166 final/2, p. 25.

([120]) See supra, section 2.1.1.3.

AI and machine-learning algorithms recognise patterns based on tell-tale signs of infringing activity, which include the following.

Vendor's profile characteristics:

- profiles selling too many brands and of different categories;
- profiles selling very similar types of products, some of them having already been identified as counterfeit or pirated goods;
- profiles that publish an instant messaging number to communicate directly with the buyers and/or links to live streaming sales of products;
- profiles that receive an unusual amount of very good feedbacks in a short period of time.

Suspicious behaviours:

- products listed for an improbably low price ('too good to be true' price for an authentic good);
- listings that have links to redirect users to websites that have been subject to takedown procedures or blocking orders;
- use of images where the brand name and logo is covered or blurred.

Comments and rating:

- comments that complain about the quality of the product, or even expressly suggest or warn that the product is a fake ([121]); or alternatively,
- positive comments that are posted from the same account multiple times, or from suspended or disabled accounts.

([121]) See infra, case No 6 in Appendix.

2.1.3 Investigation and enforcement

Along with voluntary measures developed in collaboration with online marketplaces, rights holders and law enforcement agencies adopt a series of policies and strategies to tackle IP infringement on online trading platforms. These include investigative and enforcement measures that are broader in scope and span across the whole supply chain discussed in the previous part of this report.

2.1.3.1 Monitoring and 'follow the money'

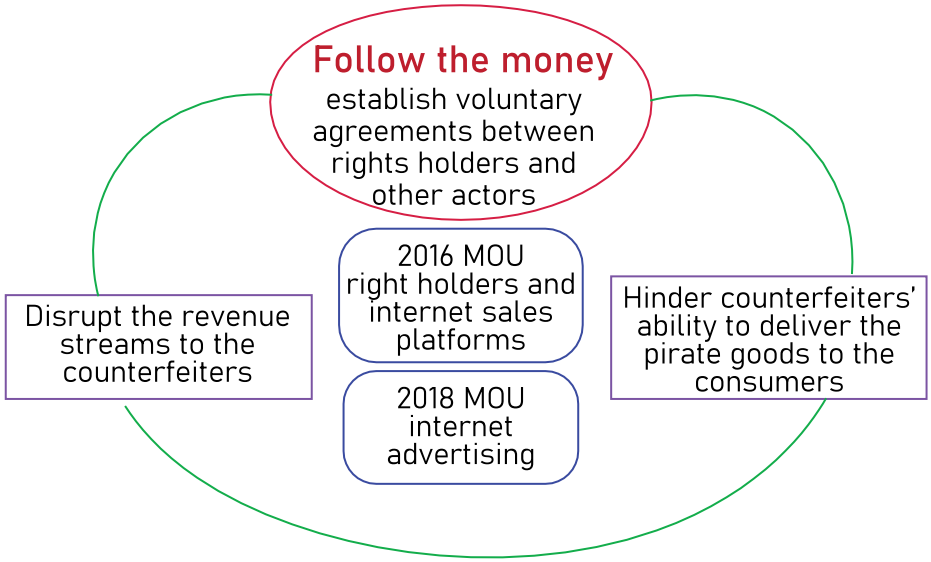
A 'follow the money' approach is generally used to tackle forms of organised crime. It consists, essentially, in monitoring and extracting information from the financial transactions involved in an illicit activity, with the purpose of collecting evidence and/or disrupting the activity. The procedures involved are complex and require cooperation between the different stakeholders involved, most importantly the payment services.

The European Commission has adopted a 'follow the money' approach in a series of initiatives aimed at disrupting the revenue streams to the counterfeiters and hindering their ability to deliver IP-infringing goods to consumers ([122]). As part of these initiatives, two voluntary agreements between rights holders and other actors have come into effect: the 2016 Memorandum of Understanding on the sale of counterfeit goods on the internet ([123]) and a second MoU on online advertising and IPR, signed in 2018 and designed to reduce advertising by legitimate brands on IPR-infringing websites and mobile applications ([124]).

([122]) European Commission, The Follow the Money Approach to IPR Enforcement – Stakeholders' Voluntary Agreement on Online Advertising and IPR: Guiding Principles.

([123]) See supra, section 2.1.1.

([124]) Memorandum of understanding on online advertising and IPR https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr_en.



It is important to observe that the sale of counterfeit and pirated goods is one of the 22 predicate offences under the sixth Anti-Money Laundering Directive ([125]). This is reflected in the due diligence systems put in place by payment services providers, which must comply with anti-money laundering legislation. As seen above ([126]), some marketplaces are also providing payment services to their vendors (and are even registered as e-money institutions), and they have to put a number of due diligences in place to monitor illegal activities, including sales of counterfeit and pirated goods. Moreover, this implies that IP-enforcement activities, as part of 'follow the money' investigations, can be carried out on the basis of money laundering.

An example of how anti-money-laundering enforcement measures can be used in the context of a 'follow the money' approach to IP enforcement, is the Swedish case 'SweFilmer' ([127]). In this case, which is about unlicensed streaming of audio-visual works, the defendant was charged with both copyright infringement and laundering the profits of the illicit activity. Since money laundering carries

([125]) Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, Article 2(1)(k).

([126]) See supra, section 1.2.2.

([127]) Hovrätten for western Sweden Case No B 3143-17, 18/03/2018. See EUIPO (2021) *International judicial cooperation in intellectual property cases* (March 2021), p. 87.

higher penalties than copyright infringement the 'follow the money' approach was allegedly 'not only instrumental to unravelling the illicit activities and the persons responsible but also essential to the use of international cooperation investigative measures' ([128]).

2.1.3.2 Customs and border checks on small packages

As seen previously in this report, an increasingly large proportion of global shipments is represented by small packages ([129]). This increase in the volume of small packages sent to consumers has been connected to an increased trade in counterfeit goods. In 2018, the OECD and the EUIPO observed that the trafficking of counterfeit goods in small packages through postal or express carrier services was a growing trend, and was becoming a significant problem in terms of enforcement ([130]).

A report by the United States Government Accountability Office (GAO) from September 2020 compares how the EU and US agencies responded to the challenge of customs checks on small packages ([131]). The report examines:

1. how selected elements of the EU and US approaches to combating counterfeit goods in small packages compare;
2. any common challenges reported by EU and US customs officials in conducting enforcement against such goods; and
3. the extent to which the US Customs and Border Protection (CBP) has taken steps to address these challenges.

([128]) Ana Nordberg and Knud Wallberg (2018) 'Intellectual Property Rights in a Digital Environment: An EU Wide Mapping of Available Legislative Enforcement Measures', *University of Copenhagen Faculty of Law Research* Paper, p. 16. Available at SSRN: https://ssrn.com/abstract=3251841.

([129]) See supra, section 1.1.1.

([130]) Trade in Counterfeit and Pirated Goods. Mapping the Economic Impact, OECD/EUIPO (2016), OECD Publishing, Paris.

([131]) United States Government Accountability Office (GAO), Report to the Chairman, Committee on Finance, US Senate 'CBP Has Taken Steps to Combat Counterfeit Goods in Small Packages but Could Streamline Enforcement', September 2020.

Differences in EU and US approaches to detecting counterfeit goods in small packages include procedures, time frames, cost sharing, and data sharing:

i. the European Union uses a streamlined procedure to destroy suspected counterfeits in small packages, whereas the US authorities are required to conduct seizure and forfeiture for all counterfeits;
ii. the EU small packages procedure uses a condensed time frame, whereas the US process includes more time for parties to respond;
iii. in the European Union, rights holders can be billed for storage and destruction, whereas those in the US are not subject to cost sharing; and
iv. in the EU, customs authorities provide data to rights holders upon request, and as appropriate after goods are destroyed, whereas in the US, the CBP is required to provide certain data to rights holders upon seizure of a good bearing a counterfeit mark.

Although the EU and US customs authorities differ in several elements regarding how they address counterfeit goods in small packages, both report that they are confronting similar issues related to the lack of data on small packages, which blocks their ability to successfully move to enforcement actions.

The CBP has taken initiatives to tackle the challenges presented by counterfeit goods in small packages. These initiatives include implementing and concluding a pilot programme that allowed for the abandonment of suspected counterfeit goods, so that such goods could be destroyed more quickly, and thereby removed from the US economy. Additionally, the CBP has begun to obtain additional data for lower-value goods in small packages that typically enter the US with little or poor-quality data about their contents, origin or destination.

Differences between EU and US approaches to combating counterfeit goods in small packages		
	EU	US
DESTRUCTION 	Streamlined procedure	Authorities are required to conduct seizure and forfeiture for all counterfeits
TIME FRAME 	The procedure uses a condensed time frame	The process includes more time for parties to respond
COST 	Rights holders can be billed for storage and destruction	Not subject to cost sharing
PROVISION OF DATA 	Customs authorities provide data to rights holders upon request, and as appropriate after goods are destroyed	Provision of certain data to rights holders upon seizure of a product bearing a counterfeit mark is required

2.1.3.3 Enforcement on the darknet

Evidence suggests that vendors of IP-infringing products and services are expanding their businesses to marketplaces operating on the darknet, primarily the TOR-network ([132]). Given the anonymity of online providers and possible affiliates, identification of darknet businesses presents specific

([132]) EUIPO (2016) *Research on Online Business Models Infringing Intellectual Property Rights – Phase 1 Establishing an overview of online business models infringing intellectual property*. 'Tor' is an anonymous networking software program which works as an add-on to web browser software and is used to view websites in the 'onion' network, i.e. allowing vendors completely anonymous use. Some 'onion' sites have been identified that provide a laundry list of illicit goods and services, such as, among others, counterfeit currency and goods. For a further elaboration on the 'Tor' function, see the analysis of Roxanne Elings and George P Wukoson, 'Going deeper into the dark net', 01/05/2014, available at https://www.lexology.com.

challenges. Moreover, 'notice and takedown' procedures, which are provided by the operators of online marketplaces and other internet service providers on the open internet, do not appear to have any application on the darknet.

Therefore, law enforcement agencies are mainly focused on shutting down these markets. As Prasad Vana and Pradeep Pachigolla demonstrate ([133]), there are three implications for law enforcement as regards closing down darknet marketplaces.

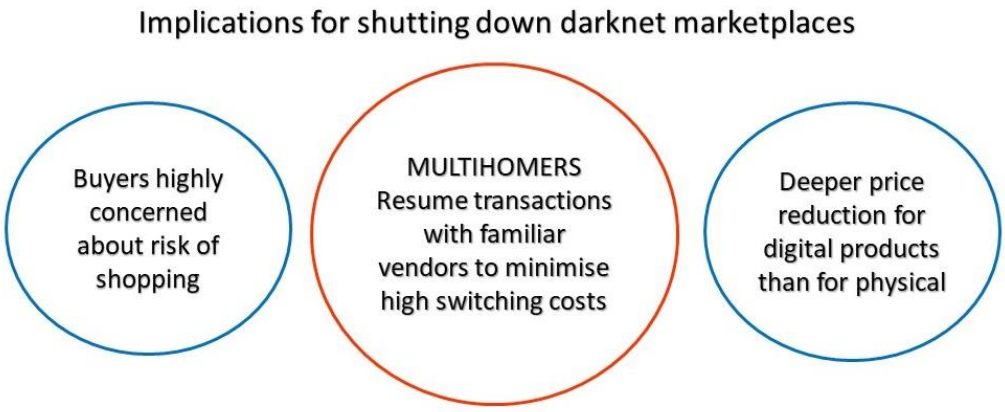
Firstly, buyers are highly concerned about the risk of shopping in a darknet marketplace after a shutdown. Given the anonymity of darknet marketplaces, it would be hard to know whether an unfamiliar market they access after a disruption is safe. Additionally, contrary to what happens in closures of illegal websites in the open internet environment, where often the publicity of the closure drives customers to search for alternative domain names of the same website, simply knowing the names of marketplaces on the darknet (such as Evolution or Agora) would not be sufficient to find them again.

Secondly, one particular way in which customers try to minimise high switching costs is by resuming transactions with vendors they were familiar with in the marketplace that has been closed. For example, 'multihomer' vendors may attract migrating customers from the closed marketplace through reduced prices. Consequently, when considering closing down either a marketplace with several vendors who 'multihome' in other marketplaces, or a marketplace where only a few vendors 'multihome', the latter alternative is recommended. In this way price reductions in other markets could be kept at a minimum after the market was closed down.

Thirdly, price reductions after disrupting a market are significantly deeper for digital products than physical products. Hence, when deciding between closing down a marketplace which has a mix of physical and digital products (such as Evolution) or a marketplace where the great majority of products sold are physical (such as Agora), the former is recommended. The reason for that is that after law

([133]) Prasad Vana and Pradeep Pachigolla, 'Do Law Enforcement Busts of Darknet Markets Deter Criminal Activity in Other Darknet Markets?' (June 2020), Tuck School of Business Working Paper No. 3474719, Available at SSRN: https://ssrn.com/abstract=3474719.

enforcement agencies shut down the marketplace that has a mix of physical and digital products, vendors in the marketplace with predominantly physical products would try to reduce their price to attract buyers.



Notwithstanding legal and technological barriers in the fight against darknet marketplaces, there have been some significant successes by law enforcement authorities against darknet marketplaces selling counterfeit goods.

- In August 2017, the US Justice Department announced that, together with other international law enforcement agencies, including Europol, 'The largest darknet marketplace in history was shut down' ([134]). The marketplace in question was AlphaBay, a web bazaar where users' identities were cloaked, and illicit goods and drugs were sold. AlphaBay was allegedly selling counterfeit goods and 'other computer hacking tools, firearms, and toxic chemicals throughout the world,' through '250 000 listings for illegal drugs and toxic chemicals,' and 100 000 other illicit items ([135]).

([134]) Colin Dwyer, 'Justice Department Announces "Largest Darknet Takedown In History"', 20/07/2017, available at https://www.npr.org.

([135]) Colin Dwyer, 'Justice Department Announces "Largest Darknet Takedown In History"', 20/07/2017, available at https://www.npr.org.

- In March 2019, a joint operation headed by OLAF (the European Anti-Fraud Office) and the Belgium Customs service in collaboration with customs services from other Member States and Europol ('Operation Postbox II'), resulted in the seizure of over 1 200 packages of counterfeit products traded on darknet marketplaces. The detentions were followed by the creation of a specialised 'cyber patrol' to raid the open web and the darknet, and identify the infringers based on profiles of vendors and shippers ([136]).

- A recent and significant operation of international law enforcement authorities against darknet marketplaces was announced by the US Department of Justice in September 2020. The case involved the arrest of hundreds of individuals worldwide operating on darknet marketplaces in the field of drugs and weapons trade. A number of darknet vendor accounts were identified and attributed to real individuals selling illicit goods on marketplaces such as AlphaBay, Dream, WallStreet, Nightmare, Empire, White House, DeepSea, Dark Market and others ([137]).

Darknet marketplaces shut down
Alphabay
Silk Road
Silk Road 2.0
Opioid

2.1.3.4 Disruptive technologies

Tracking darknet users is of utmost importance in the fight against online counterfeit trade. Identifying the real-world and real-life account owners behind the vendors – and cryptocurrencies accounts – by correlating transactions with other actions of connected individuals, tracked through traditional investigatory techniques, can give a major boost to enforcement. In the US, the Advanced Research

([136]) EUIPO (2020) *Status report on IPR infringement*, June 2020, p. 33.

([137]) US Department of Justice, 'International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and over $6.5 Million. Darknet Narcotics Vendors Selling to Tens of Thousands of US Residents Charged', 22/09/2020, available at https://www.justice.gov.

Projects Agency has developed a search technology known as Memex, which can search the darknet for law enforcement purposes, such as combating human trafficking ([138]). An analogous use could be adopted for online sales of counterfeit goods.

The impact of so-called disruptive technologies on IP protection, infringement and enforcement, has been analysed by the EUIPO in a discussion paper published in 2020 ([139]). Such technologies include artificial intelligence, robotics, blockchain, 3D printing, nanotech and augmented reality. They have four stages of application in relation to IP: exploration, conversion, weaponisation and monetisation.

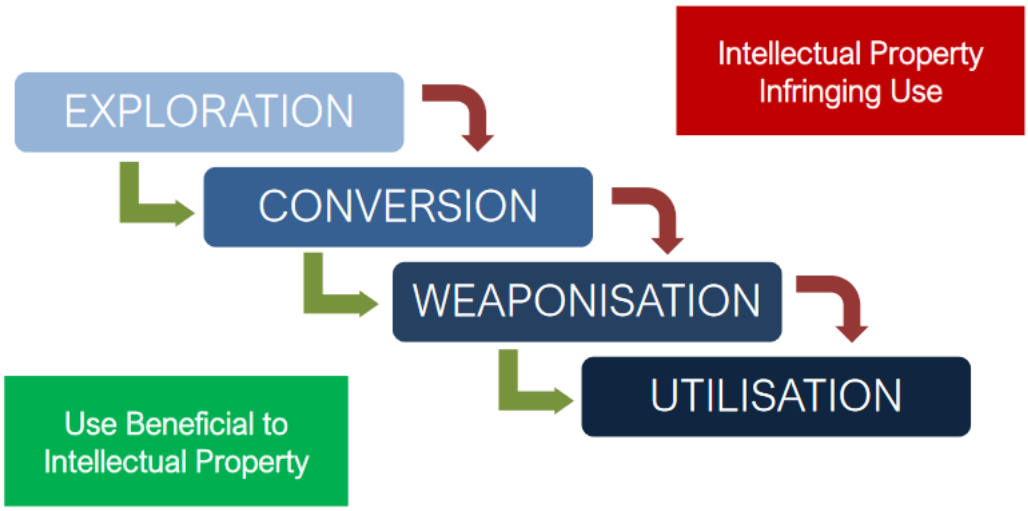


Figure 5 – Simplified version of the 'Intellectual Property Tech Chain'

Through this four-step methodology, called 'The Intellectual Property Tech Chain', the new technologies are tested and assessed with regard to whether they can serve for the protection, infringement and enforcement of IP rights. It is noteworthy to observe that the abovementioned disruptive technologies can be potential tools for both the protectors and enforcers of IP rights as well as for the IP infringers who are able to produce, market and distribute counterfeit goods and services

([138]) https://www.darpa.mil/about-us/timeline/memex.

([139]) EUIPO (2020) 'Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper', available at https://euipo.europa.eu.

more effectively. The above methodology is the process that will distinguish how, and to what extent, each technology can serve one side or the other.

2.2 VENDORS' LIABILITY: SELECTED CASE-LAW FROM EU MEMBER STATES

Vendors on online marketplaces can be found liable of infringement of IP rights when they offer for sale counterfeit or pirated goods, as well as goods that infringe IP rights on other grounds, including authentic goods imported into the EEA without rights holder's authorisation ([140]). The legal basis to determine infringement is to be found in both EU and national legislation. As far as EU-harmonised IP rights are concerned, the most important instruments are the Regulations on, respectively, European Union Trade Marks ([141]) and Community Designs ([142]), and the Directives that constitute the *acquis* on copyright and related rights ([143]). The scope of these provisions has been subject, in turn, to extensive harmonisation by the CJEU.

GOODS ON SALE	MAIN LEGAL BASIS TO DETERMINE INFRINGEMENT
Counterfeit goods: fakes and replicas	EUTM Regulation 2017/1001, Article 9(2)(a)
Pirated goods (physical)	InfoSoc Directive 2001/29, Articles 2 and 4 and Article 6(2) Community Designs Regulation 6/2002, Article 19
Pirated goods (digital)	InfoSoc Directive 2001/29, Articles 2 and 3 Computer Programs Directive 2009/24, Articles 4 and 7
Confusingly similar goods	EUTM Regulation 2017/1001, Article 9(2)(b)
Goods exploiting a famous brand	EUTM Regulation 2017/1001, Article 9(2)(c)
Grey-market goods	EUTM Regulation 2017/1001, Article 9(3)(c) and Article 15 InfoSoc Directive 2001/29, Article 4 Community Designs Regulation 6/2002, Articles 19 and 21

IP infringement in the EU can result in civil and criminal liability. This section presents a selection of judgments from national courts on criminal proceedings against vendors of IP-infringing goods on

([140]) See supra, section 1.2.1.

([141]) Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification).

([142]) Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs.

([143]) In particular, Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, and Directive 2009/24EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (codified version).

third-party online marketplaces. While civil liability for IP infringement is broadly harmonised at EU level ([144]), criminal liability remains the competence of national legislators. Under the provisions of the TRIPs Agreement, member states 'shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale' ([145]). Such procedures are available in all EU Member states, where national criminal law requires a degree of wilful intent (or *mens rea*) and a commercial scale infringement for an act to be criminally sanctioned. However, national jurisprudence constructs these criteria differently ([146]).

2.2.1 Sale of pirated software on an auction marketplace

The case **Ranks and Vasiļevičs v Microsoft** ([147]), referred to previously in this report ([148]), arose in Latvia. Two defendants were accused of selling pirated copies of Microsoft software on eBay. Civil proceedings were brought on several counts, including copyright and trade mark infringement related to the reselling of 32 backup copies of Microsoft Windows operating systems. A separate count indicted the defendants for copyright infringement related to the illegal reselling of more than 3 000 Microsoft software products. Criminal charges were brought for the unlawful resale of copyright-protected products, for trade mark infringement, and for engaging in an entrepreneurial activity without a licence.

The case resulted in five court rulings, each one partly adding to or modifying the interpretation of the defendants' criminal responsibility for the elements highlighted above. During the proceedings, the CJEU was also asked to provide a preliminary ruling on the application of the exhaustion of rights rule to backup copies of software. In its (so far) only decision in a case on vendor accounts on third party trading platforms, the CJEU clarified that backup copies may only be made and used by the legitimate

([144]) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

([145]) TRIPs Agreement, 1994, Article 61.

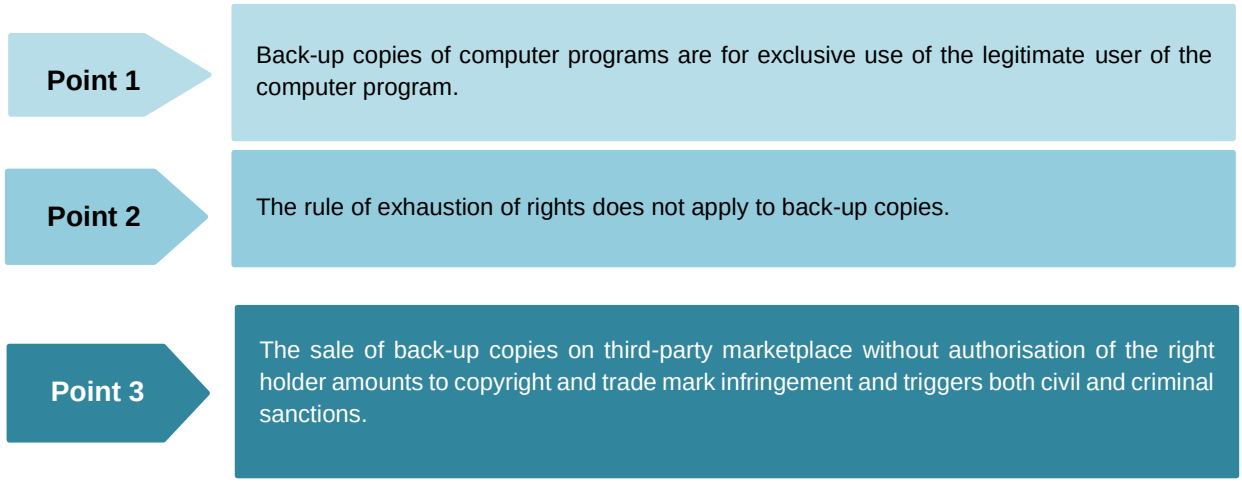
([146]) EUIPO (2018) *Study on legislative measures related to online IPR infringements*, p. 65.

([147]) Court of Cassation (Latvia), 23 February 2018.

([148]) See supra, section 1.2.1. The business model related to this case is presented in appendix, case no. 11.

owner of the computer program and cannot be sold to a third party ([149]) Both defendants were found guilty for the sale of 36 backup copies, but were acquitted from the charge of the sale of 3 000 copies, as the Court was not presented with sufficient evidence. They were sentenced to 6 months imprisonment. Microsoft was awarded EUR 7 000 damages for the sale of 36 backup copies.

Ranks and Vasiļevičs v Microsoft, 23 February 2018



In a case from the **Frankfurt am Main Higher Regional Court** on 12 December 2016 (the names of the parties are not provided), the court ruled that a punishable trade mark infringement already exists if data carriers are provided with software certificates of authenticity without there being a physical connection. This decision means that even the mere addition of the certificates constitutes a trade mark infringement, since it is a new compilation.

The defendants purchased used original equipment manufacturer (OEM) versions and attached software authenticity certificates to them. This is software available under a licence agreement from the software manufacturer. The computer manufacturer acquires the right to sell the software in packages based on that licence agreement, by installing it on the hardware it manufactures. The defendants purchased the DVDs from a vendor in England, and sixty percent of the certificates of

([149]) Ranks and Vasiļevičs v Microsoft (12/10/2016, C-166/15, EU:C:2016:762, § 43).

authenticity came from China. However, they knew that the vendor from China also dealt in illegal software. The defendants purchased forty percent of the certificates of authenticity in Germany and Italy.

There was a division of labour among the defendants, with one doing the administrative and clerical work and making occasional sales, while the other made the purchases and sales. The defendants purchased the products in tranches of various sizes, and then assembled the software from various units. In addition to purchase invoices, the defendants were unable to provide proof of origin or other supporting documentation and did not offer such documentation when reselling. Frequently, the software was purchased for cash. The defendants were also aware that the prices for the purchased products were conspicuously low, and they in turn sold for far less than the normal market price for the product. Although they hoped that they were not purchasing illegal and counterfeit goods, they were aware that the products they were selling were protected by trade mark law. They then sold the software via the eBay platform. However, the certificates of authenticity did not belong to the OEM versions sold, but came from other computer programs.

The Court classified this action as a punishable trade mark infringement under the German Trademark Act. From a legal point of view, the defendants modified the sold computer software to such an extent that a new compilation existed, since they provided it with third-party certificates of authenticity. The trade mark owner concerned did not have to accept this, because a trade mark always functions as both an origin and a guarantee. This legal requirement was no longer fulfilled by the new combination of data carrier and certificate of authenticity. A physical connection was not necessary, because the rights holder had a great interest in ensuring that only the data carriers it puts on the market itself were provided with the certificates of authenticity that were the subject of the complaint. By attaching the certificates of authenticity to the data carriers, the (incorrect) impression was created that the right holder had authorised and certified the software. Because of this certificate of authenticity, consumers placed increased trust in the product.

By distributing the disputed software with third-party certificates of authenticity, the defendants had used a protected mark in a distinctive manner. By doing so, they unjustifiably distinguished their own product from similar products of foreign origin. Therefore, there was a likelihood of confusion under the German Trademark Act. The protected signs were used without the consent of the rights holder. Since the goods in question were counterfeit, it can be assumed that the rights holder did not consent

to such use of its protected mark. For the operating systems, which could not be established as counterfeiting, exhaustion of the trade mark right could theoretically have occurred by way of the first sale within the EU/EEC, on the basis of the licence agreement.

Frankfurt a/Main Higher Regional Court, 12 December 2016

Point 1	A punishable trade mark infringement already exists if data carriers are provided with counterfeit software certificates of authenticity.
Point 2	A vendor liability is established when the defendant is unable to provide proof of origin of products or other supporting documentation and does not offer such documentation when reselling the counterfeit products.
Point 3	Distributing pirated software with third-party certificates of authenticity, a vendor uses a protected mark in a distinctive manner, and by doing so, he unjustifiably distinguishes its own product from similar products of foreign origin. Thus, there is a likelihood of confusion under the German Trademark Act.

2.2.2 Sale of counterfeit spare parts and pirated diagnostic software on an auction marketplace

The Higher Regional Court in Koblenz, with its ruling on 15 January 2014 (the names of the parties are not provided), ruled on two joined cases with the same defendant: the former concerning unauthorised commercial exploitation of copyright protected works, and the latter concerning commercial criminal trade mark infringement based on the German Trademark Act.

The defendant was charged with obtaining 'Mercedes Benz Star Diagnostics' systems that were copied commercially from China on a large scale, and with selling these systems via the internet to customers in Germany and abroad, together with the diagnostic software 'Xentry Diagnostics' and 'Xentry DAS', the repair database 'WIS/ASRA', and the spare parts database 'EPC'. The sale of these products had taken place mainly via the eBay platform under the dealer name 'newcarmedia'.

Access to the plaintiff company's original software's content was supposed to be technically protected by a so-called 'start key', which could be purchased for a limited period of time. This protection mechanism was said to have been circumvented in the distributed devices by a pre-installed valid start key and new valid start keys that were generated by the device when the previous one expired.

In addition, the defendant was alleged to have made large-scale purchases of counterfeit car radio systems with GPS navigation from China, and to have resold them via the eBay platform. In the sales offers, the device was said to have been advertised with the VW trade mark shown on the display and to have been described as 'GPS Navigation VW Golf Skoda Seat MD211S DVD GPS DVB-T'. After the devices were switched on, the 'VW', 'Seat' or 'Skoda' brand logo was allegedly visible on its display, depending on the vehicle type specified as compatible with the device.

Higher Regional Court Koblenz, 15 January 2014

Point 1	The vendor/defendant has purchased, on a large scale, counterfeit car radio systems with GPS navigation from China, and then resold them via the eBay platform.
Point 2	In reaching its ruling, the Court considered whether the potential preliminary measures, either the forfeiture of value replacement or an arrest, would cause the defendant a considerable disadvantage.
Point 3	The German Local Court ordered an injunction *in rem* against the defendant's assets in the amount of EUR 130 791.18 to secure the civil claims of the injured parties arising from the criminal acts.

2.2.3 Sale of counterfeit clothing on an auction marketplace

On 11 November 2007, **the District Court of Mühlhausen** (the names of the parties are not provided), ruled on a case concerning the production and sale of counterfeit clothing products on the eBay platform.

The defendant, having been registered as a member of the eBay platform, registered an eBay shop, through which he intended to sell fan articles. He ordered T-shirts, sweaters, and girly blouses, on which the registered word/figurative mark 'Böhse Onkelz' was attached. The T-shirts were then offered for sale on the eBay platform and sold individually. The defendant was not entitled to use the aforementioned word/figurative mark, protected by registration in the trade mark register of the German Patent and Trademark Office, because the trade mark owners had not agreed to this use.

The defendant knew this. Earlier, he had also tried to obtain authorised trade marked goods from other owners of well-known trade marks in the music industry, but he had to give up because the authorised branded goods were too expensive. The defendant chose the band 'Böhse Onkelz' because he knew that textiles bearing their brand could be sold easily and profitably.

After a while, the defendant decided to produce the textiles he was selling on eBay himself. To this end, he bought a textile printing carousel and drying tunnel on eBay. After deducting additional costs for personnel, rent and printing material, the defendant achieved a gross profit of approx. EUR 5 000.00 from the EUR 24 215.00 generated from the sale of goods.

The defendant, after discovery by the German authorities, admitted, among other things, that he wanted to initiate the permanent production of counterfeit branded goods by purchasing the printing press.

The discovery court's examination revealed that the trade mark owners had not consented to the use of the trade mark by the defendant. The trade mark used in the online sales was identical to or at least similar to the protected trade mark. In addition to the brand identity, product identity was also involved, because the protected brands related to a specific protected class (textiles). With regard to the required product identity, it was sufficient that the product belonged to the protected class. Complete identity with products already sold by the authorised users of the brand was not required.

The Court, in its legal reasoning, tried to draw an analogy between this case and other cases with similar facts. The Court referred to another case, in which it was found that obtaining counterfeit money with the intention of selling it at a favourable opportunity and the subsequent realisation of this intention as two separate acts is to be regarded as an act within the meaning of the relevant provision of the German Criminal Code. Likewise, the German Constitutional Court decided in the area of copyright infringement for the relationship between duplication and distribution. If these principles were to be transferred to the current case, it would mean that the sale of clothing items in violation of the 'Böhse Onkelz' brand, as shown in the indictment, could not be viewed as a majority act with regard to every item sold, nor as a violation of the German Trademark Act. The individual sales transactions related to the unlawfully trade marked goods previously procured or manufactured with the intention of then selling them, are bracketed into a single action.

In this case, there were a total of six actions, ordering, printing, placing, selling, printing their own clothing, and selling again on the eBay platform. Each of these actions was to be punished according to the German Trademark Act with imprisonment of up to 5 years or a fine. Finally, considering the defendant's credible confession of his actions, he was fined, for all the actions, with an overall fine of 160 daily rates of EUR 10.00 each, and all the instruments and textiles were confiscated.

District Court of Mühlhausen, 11 November 2007

Point 1	A vendor selling unauthorised products on the eBay platform was also the manufacturer of counterfeit products.
Point 2	The trade mark owners had not consented to the use of the trade mark by the defendant, and the trade mark used in the online sales was identical to or at least confusingly similar to the protected trade mark.
Point 3	The Court found that in this case there were a total of six illicit actions on the eBay platform: ordering, printing, placing, selling, printing their own clothing, and selling again. Each of these actions was to be punished according to the German TradeMark Act either with imprisonment of up to 5 years or with a fine.

2.2.4 Sale of counterfeit luxury goods from an online shop

On 22 December 2016, the **Helsinki District Court** (the names of the parties are not available), ruled on a case concerning the Finnish Criminal Code as well the Finnish Trademarks Act.

In this case, counterfeit products were sold from a specific online shop. The defendant imported counterfeit luxury bags from Asia, and sold them in their own online shop.

The District Court found that it is general knowledge that counterfeit products are made in Asia and sold considerably cheaper than the authentic products. According to the Court, it was undisputed that the products were counterfeit and were also sold in the defendant's online shop at a considerably cheaper price than that of the authentic products. Based on the circumstances, the defendant must have known the products were counterfeit. The Court concluded that because the products were sold

through the defendant's online shop, and considering the volume of the activity, they were guilty of committing an intellectual property offence.

Helsinki District Court, 22 December 2016

Key point

Criminal liability could be established on the following objective grounds: a) general knowledge that counterfeit products are made in Asia, b) counterfeit products are sold considerably cheaper than the authentic products, and c) the infringer's activity generated considerable volume.

2.2.5 Sale of pirated design articles on an auction marketplace

Another Finnish Court, the **District Court of Ylivieska**, ruled on 1 April 2016 on a case concerning the Finnish Trademarks Act, the Finnish Copyright Act, and the Criminal Code of Finland.

In this case, the defendant had sold in an online auction marketplace Sony PlayStation DualShock controllers, controller batteries, PlayStation steering wheels, and bags that incorporated a trade mark owned by Marimekko Oyj and which resembled bags made by Marimekko Oyj.

The District Court ruled that the defendant had known that the bags were counterfeit. But the Court did not consider that there was evidence that the volume of the defendant's activity was sufficient to constitute an intellectual property offence, as defined by Finnish law. However, the Court did find that the defendant had acted for profit and in violation of the Copyright Act in a manner conducive to causing considerable detriment or damage to Marimekko Oyj. The defendant was therefore found guilty of a copyright offence. Regarding the PlayStation controllers, the District Court found the defendant guilty of trade mark infringement of Sony's trade mark 'DualShock'. The Court dismissed the case regarding the controller batteries and steering wheels.

Ylivieska District Court, 1 April 2016

Point 1	Although the defendant was found to know that the products sold on an online auction marketplace were counterfeited, the Court did not consider that there was evidence that the volume of the defendant's activity was enough to constitute a criminal offence.
Point 2	Nevertheless, the Court did find the defendant guilty for violating the Copyright Act as well the Trademark Act. The defendant had acted for profit in a manner conducive of causing considerable detriment or damage to the copyright holder as well as to the trade mark holder.

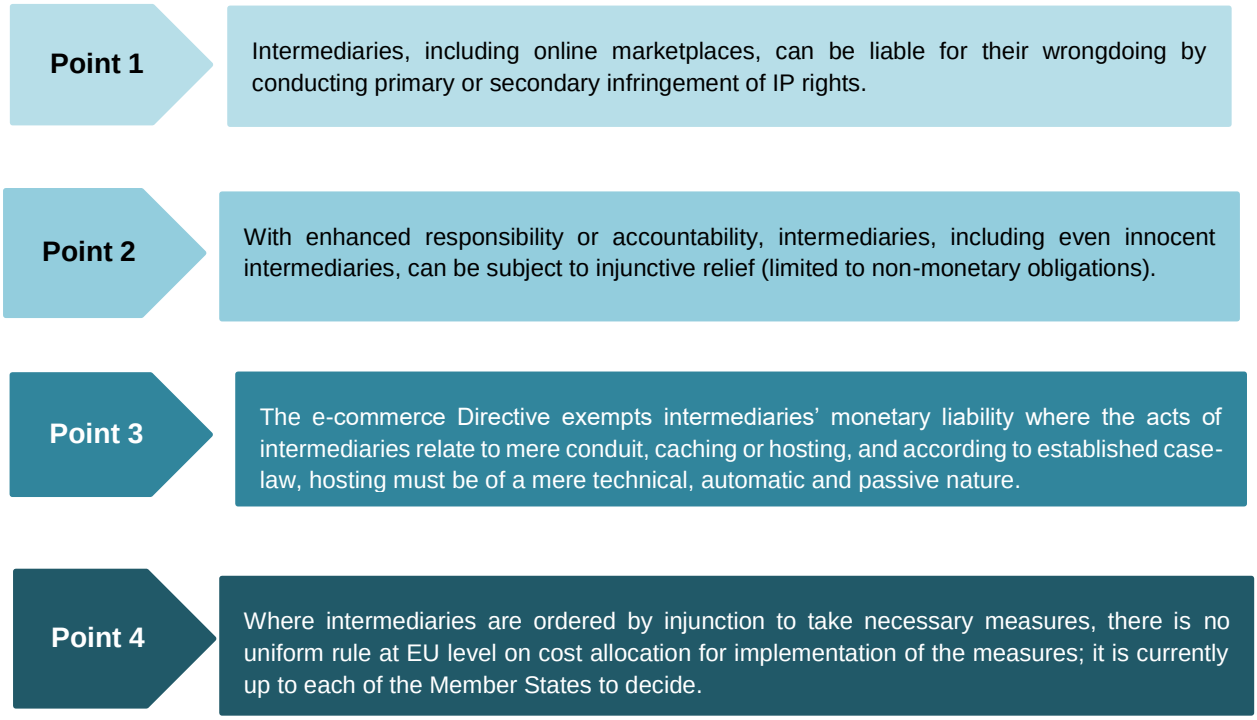
On 3 March 2020, in Hungary, the **Municipal Court of Appeals** (the court of appeals in Community design cases), ruled on a case concerning Council Regulation No 6/2002 on Community designs and the Hungarian Act XLVIII of 2001 on design protection.

In this case, the vendor/defendant was selling gift boxes that resembled the registered Community designs of the plaintiff. The vendor's website, as well as the links directing to the plaintiff's Instagram page and YouTube channel, included visual advertisements that called for the order of the gift boxes, if purchasers ordered other products as well. The second defendant was allegedly the 'face' of the advertisements for example they made endorsements of the first defendant's products). The plaintiff claimed that both defendants had infringed its Community design rights by making, offering, putting on the market, and stocking the gift boxes.

The court of appeals found that the plaintiff's registered boxes and first defendant's boxes should be compared, and that the differences should be the focus of this comparison rather than the similarities. The colours, shape, exact sizes, proportions of various parts, and accompanying texts all had relevance in this analysis. The court of appeals agreed with the trial court that the first defendant's gift boxes showed significant differences from the plaintiff's boxes. A purchaser having a higher degree of knowledge about the relevant products would easily be able to differentiate between them. The court of appeals also stated that the second defendant did not 'use' the first defendant's boxes, even though they endorsed the products.

2.3 INJUNCTIONS AGAINST INTERMEDIARIES

Key Points



As seen in the previous sections, rights holders and law enforcement agencies can act against vendors directly, via legal actions, or through non-judicial measures, developed in collaboration with online marketplaces. However, these actions may not always be available, or may not be effective in tackling the infringement. For example, judicial proceedings against vendors may not be pursued because the identity of the infringers is unknown, or because they are based in remote jurisdictions ([150]). Likewise, non-judicial measures such as effective NTD procedures may not be successful in stopping the infringement, or may not be available in the first place ([151]). It must be borne in mind that the EU legal framework (including both 'hard' and 'soft' law) creates strong incentives for marketplaces to actively collaborate in the fight against the sale of IP-infringing goods. However, these collaborative measures are voluntary and principally rely on business decisions.

([150]) See discussion infra, section 2.4.

([151]) This is the case of 'rogue' marketplaces operating on the darknet (see supra, section 2.1.3.4).

This section discusses the judicial remedies available to rights holders to seek redress from online marketplaces and other intermediaries along the supply chain. These include, in particular, warehouses, advertising platforms, payment services and shipping services ([152]). The available judicial remedies consist of injunctions, which may be granted by the judicial authority even when the intermediary is not liable for the infringement or is exempt from liability.

2.3.1 Legal basis for injunctions against intermediaries

Liability of online marketplaces and other intermediaries arises where they engage in an act that constitutes infringement of an IP right, such as those conferred by the registration of a trade mark or a design in the EU ([153]). Moreover, liability may also arise when they contribute to an infringing act committed by their users. This latter form of liability, commonly termed 'secondary', 'indirect' or 'accessory' liability, is not harmonised by EU law and is left to the legislation of Member States ([154]). However, online intermediaries may benefit from the exemptions to liability laid down by the e-commerce directive for 'Information Society Service Providers' (ISSPs) ([155]).

([152]) See supra, section 1.3. Major operators of online marketplaces offer some of all of those services to their customers (see supra, section 1.2.2).

([153]) Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark [2017] OJ L154/1, Article 9-16, and Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks (Recast) [2015] OJ L336/1, Articles 10-15; Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, Article 19.

([154]) Matthias Leistner, 'Structural Aspects of Secondary (provider) Liability in Europe' (2014), *JIPLP* 75, Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) p. 12-14; Frederick Mostert 'Intermediary Liability and Online Trade Mark Infringement: Emerging International Common Approaches', in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020), p. 369; Richard Arnold, 'Intermediary Liability and trade mark infringement: a common law perspective' in ibid., p. 406. For a comparative analysis of secondary liability in EU Member States and internationally see Graeme Dinwoodie (ed), *Secondary Liability of Internet Service Providers* (Springer 2018). For a comparative analysis across EU member states see European Observatory on Counterfeiting and Piracy, *Injunctions in Intellectual Property Rights*.

([155]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1 (e-commerce Directive), Articles 12-15.

Irrespective of primary or secondary liability, and notwithstanding the e-commerce special exemptions from secondary liability, intermediaries may still be subject to injunctive reliefs aimed at terminating or preventing an infringement taking place on their services, or at obtaining information about an infringer. Under EU law, these remedies are available against all 'intermediaries whose services are used by third parties to infringe an intellectual property right' ([156]). The notion of 'intermediary' encompasses a wide range of entities that provide services to third parties, and includes both online and physical services ([157]). A noteworthy point is that this injunctive relief is also available against innocent intermediaries. The basis for such injunctive relief has been described as a principle of enhanced responsibility or 'accountability', which imposes certain obligations on intermediaries irrespective of any liability ([158]). The underlying rationale for imposing enhanced responsibility on intermediaries is that, as stated in Recital 59 to the Information Society Directive ([159]), in the digital environment, services of intermediaries are widely used for infringing activities and intermediaries are best placed to bring infringing activities to an end. In the same vein, Article 11 of the Enforcement Directive ([160]) provides legal grounds for injunctions against intermediaries by stating that Member

([156]) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L195/16, Article 11. See also, in relation to copyright infringement, Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Article 8(3).

([157]) An economic operator is construed as an 'intermediary' where 'it provides a service capable of being used by one or more other persons in order to infringe one or more intellectual property rights, but it is not necessary that it maintain a specific relationship with that or those persons' (07/07/2016, C-494/15, Tommy Hilfiger, EU:C:2016:528, § 23). 'The fact that the provision of sales points concerns an online marketplace or a physical marketplace such as market halls is irrelevant in that connection' (07/07/2016, C-494/15, Tommy Hilfiger, EU:C:2016:528, § 29). See also AG Opinion in Case C-567/18: 'If it is ultimately found that the defendants [Amazon etc.] have not used the trade mark, their liability could still be analysed either under Directive 2000/31/EC […], if they act as e-commerce intermediaries, or under Directive 2004/48/EC' (28/11/2019, C-567/18, COTY GERMANY, EU:C:2019:1031, Part 2, § 3).

([158]) See Martin Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (Cambridge University Press 2017).

([159]) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.

([160]) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L195/16.

States shall also ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right.

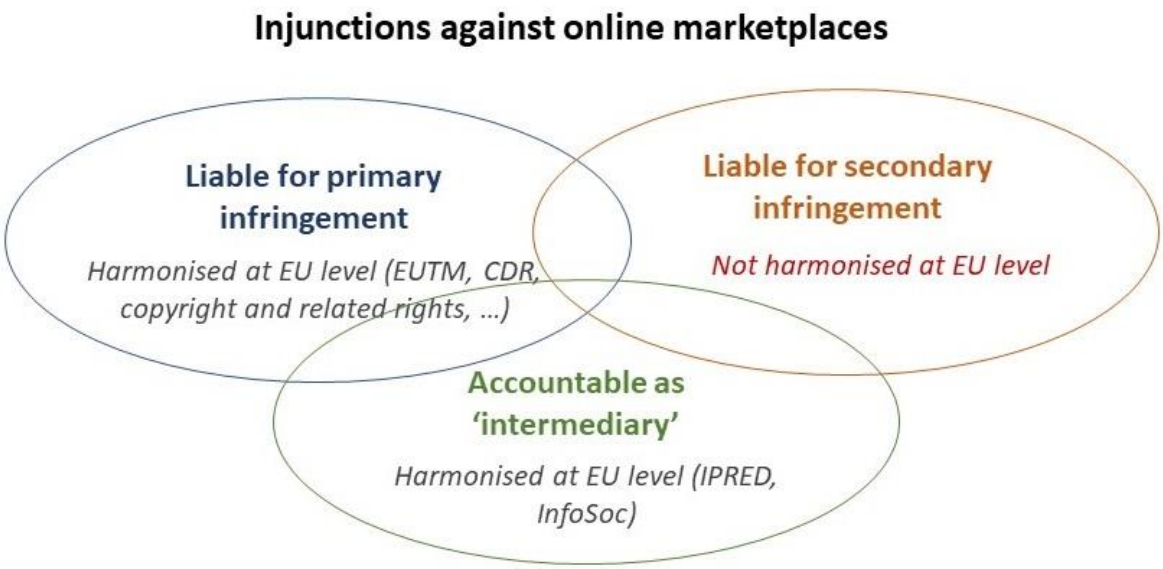


Figure 6 – The threefold legal basis for injunctions in the EU

2.3.2 Primary and secondary liability for trade mark infringement

Liability of online marketplaces may arise in the context of both primary and secondary infringement, depending on the types of acts conducted as intermediary and the degree of involvement in the transaction ([161]).

In acts in relation to registered trade marks, **primary infringement** depends on the notions of 'use in the course of trade' and use 'in relation to goods or services' ([162]). According to settled case-law, a trade mark is used 'in the course of trade' where it occurs 'in the context of commercial activity with a

([161]) Carina Gommers and Eva De Paw, 'Liability for trade mark infringement of online marketplaces in Europe: are they "caught in the middle"?', *JIPPL&P*, 2020, Vol. 15, No. 4, p. 276.

([162]) Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification), Article 9(2).

view to economic advantage and not as a private matter' ([163]). Moreover, the use is 'in relation to goods of services' whenever a 'link' can be established between the sign and the goods or services. This requires 'at the very least' that the operator 'uses the sign in its own commercial communication' ([164]). This was found to be the case where an operator of an auction marketplace used a third party's trade mark as a keyword in an online advertising platform to promote the offerings made by vendors on its marketplace ([165]). However, the purpose of such 'keyword use' is crucial: no link can be established when the marketplace uses a keyword corresponding to a third party's trade mark to promote **its own marketplace services** (where those services are not identical or similar to the goods or services of the trade mark owner) ([166]). Moreover, in relation to other ancillary services provided by online marketplaces, no 'link' can be established when the intermediary provides purely technical or logistical solutions, such as packaging ([167]) or warehouse services ([168]). In 'Coty Germany v Amazon' the CJEU has recently confirmed that 'creating the technical conditions necessary for the use of a sign and being paid for that service' does not itself amount to 'use' of the sign ([169]). In that particular case, the Court found that the provision of storage facility for goods which infringe trade mark rights, 'without being aware of that infringement', must not be regarded as an act of storing those goods for the purpose of putting them on the market, where the operator does not, itself, pursue those aims, namely offering or putting the goods on the market ([170]).

When an online marketplace is not liable for trade mark infringement it may be still be subject to **secondary liability** based on other rules of law, such as general laws on tortious liability. In most EU Member States such liability can be established if the operator has 'contributed' to the infringing act,

([163])12/11/2002, C-206/01, Arsenal, EU:C:2002:651, § 40.

([164]) 23/03/2010, C-236/08 - C-238/08, Google-Louis Vuitton, EU:C:2010:159, § 56.

([165]) 12/07/2011, C-324/09, L'Oréal-eBay, EU:C:2011:474, § 85-97.

([166]) 12/07/2011, C-324/09, L'Oréal-eBay, EU:C:2011:474, § 89-90. In case of non-identical or confusingly similar goods or services, the 'keyword use' may still be subject to scrutiny as a possible infringement of Article 9(2)(c) of the EUTM Regulation (enhanced protection for trade marks with reputation).

([167]) 15/12/2011, C-119/10, Red Bull, EU:C:2011:837.

([168]) 16/07/2015, C-379/14, BACARDI, EU:C:2015:497.

([169]) 02/04/2020, C-567/18, COTY GERMANY, EU:C:2020:267, § 43.

([170]) 02/04/2020, C-567/18 COTY, GERMANY, EU:C:2020:267,, § 53.

in the sense that it has acted negligently or incorrectly, and a causal link can be established between their conduct and the damage suffered by the trade mark owner ([171]).

2.3.3 e-commerce exemptions from liability

Online intermediaries may be exempted from liability to an extent that they act within the scope of the e-commerce Directive ([172]). Articles 12-15 of the e-commerce Directive provide a set of exemptions (safe harbours) ([173]) for Information Society Service Providers (ISSPs). The exemptions offered by the e-commerce Directive are limited to monetary liability. Therefore, ISSPs can still be subject to injunctions such as orders by courts or administrative authorities that require the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it ([174]).

An ISSP is any natural or legal person providing an information society service ([175]), which spans a wide range of economic activities taking place online ([176]). The CJEU established that various types of activities can fall within the definition of an information society service, and these include, inter alia, selling goods online ([177]) and operating an online marketplace that facilitates relations between vendors and buyers of goods ([178]). The Court has also clarified that no specific contractual relationship with the end-user is required for the supplier of these services to qualify as an intermediary ([179]).

([171]) Carina Gommers and Eva De Paw, 'Liability for trade mark infringement of online marketplaces in Europe: are they "caught in the middle"?', *JIPPL&P*, 2020, Vol. 15, No 4, p. 278.

([172]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1 (e-commerce Directive).

([173]) For discussion of the origin of the term 'safe harbour', see Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) p. 377-78.

([174]) Recital 45 to e-commerce Directive.

([175]) e-commerce Directive, Article 2(b).

([176]) Recital 18 to e-commerce Directive.

([177]) However, the supply of goods following the online sale of goods is not covered within the meaning of information society services (02/12/2010, C-108/09, Ker-Optika, EU:C:2010:725, § 23-40.

([178]) 12/07/2011, C-324/09, L'Oréal-eBay,EU:C:2011:474, § 109.

([179]) 27/03/2014, C-314/12, UPC Telekabel Wien, EU:C:2014:192, § 32-35.

Similarly, it is not necessary to provide services beyond 'basic' internet services, as long as they can be used by third parties to infringe an IP right ([180]).

ISSPs are not liable for mere conduit ([181]), caching ([182]) and hosting ([183]), and no general obligation to monitor, or to actively seek facts or circumstances indicating illegal activities is imposed ([184]). Of those exemptions, the hosting exemption is certainly the most important and contentious area, and the one that applies to all the categories of online marketplaces discussed in the previous chapters ([185]).

2.3.3.1 Passive or active role

Pursuant to Article 14 of the e-commerce Directive, ISSPs providing storage of information (hosting) are not liable for the information stored at the request of a recipient of the service. The scope of an ISSP's activity, in respect of storage of information, must be of a merely technical, automatic and passive nature ([186]). In effect, if ISSPs play 'an active role of such a kind as to give it knowledge of, or control over, the data stored' ([187]), they will be unable to benefit from the hosting exemption. The CJEU further elaborated the meaning of an active role in 'L'Oréal v eBay', by holding that 'where the operator has provided assistance that entails, in particular, 'optimising the presentation of the offers for sale in question or promoting those offers', it must be considered not to have taken a neutral position between the customer/vendor concerned and potential buyers, but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those sale offerings ([188]).

([180])19/02/2009, C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten, EU:C:2009:107, § 43.

([181]) e-commerce Directive, Article 12

([182]) e-commerce Directive, Article 13

([183]) e-commerce Directive, Article 14

([184]) e-commerce Directive, Article 15.

([185]) Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) p. 401-409.

([186]) Recital 42 to e-commerce Directive.

([187]) 23/03/2010, C-236/08 - C-238/08 Google-Louis Vuitton, EU:C:2010:159, § 120.

([188]) 12/07/2011, C-324/09, L'Oréal-eBay, EU:C:2011:474, § 116 (emphasis added).

2.3.3.2 Knowledge of illegal activity

In order to benefit from liability exemptions, the following conditions must be further met. First, ISSPs must not have actual knowledge of illegal activity or information, and, as regards claims for damages, must not be aware of facts or circumstances from which the illegal activity or information is apparent ([189]). And upon obtaining such knowledge or awareness, they must act expeditiously to remove, or to disable access to, the information ([190]).

In relation to the assessment of ISSPs' knowledge of illegal activity or information, the CJEU clarified that it is sufficient for ISSPs to have been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1)(b) of the e-commerce Directive ([191]). In effect, where ISSPs could have uncovered an illegal activity or illegal information, as the result of an investigation undertaken on its own initiative, as diligent economic operators, it is likely that they would be deemed to have been aware of the illegalities ([192]). This also applies where ISSPs are notified of the existence of such an activity or such information; however, given that the notification can be insufficiently precise or inadequately substantiated, this will not automatically preclude the hosting exemption ([193]).

The scope of proactive investigation to detect potentially infringing content has been addressed by national courts in Germany and the Netherlands in cases involving Stokke AS. A Dutch court of appeal found that an online marketplace having a 'neutral' role could not be expected to proactively investigate all listings advertising Stokke chairs, since 95 % of Stokke products traded through the marketplace were legitimate. Such an expectation would be disproportionate and would constitute a barrier to trade, since the marketplace already had NTD procedures in place ([194]). Similarly, the

([189]) e-commerce Directive, Article 14(1)(a).

([190]) e-commerce Directive, Article 14(1)(b).

([191]) 12/07/2011, C-324/09, L'Oréal-eBay, EU:C:2011:474, § 120.

([192]) 12/07/2011, C-324/09, L'Oréal-eBay, EU:C:2011:474, § 122.

([193]) 12/07/2011, C-324/09, L'Oréal-eBay, EU:C:2011:474.

([194]) Court of Appeal Leeuwarden, 22 May 2012, Stokke AS v Marktplaats BV. See Carina Gommers and Eva De Paw, 'Liability for trade mark infringement of online marketplaces in Europe: are they "caught in the middle"?', *JIPPL&P*, 2020, Vol. 15, No. 4, p. 281-282.

German Supreme Court ruled that an investigation assisted by image-recognition software, but requiring a manual check for each and every listing, would be 'unreasonable for the defendant in view of the effort involved' ([195]).

2.3.3.3 Expeditious removal of information

There is no statutory definition of what is required from an ISSP to 'act expeditiously' upon receiving knowledge of an infringement. The period for responding depends on the circumstances, including the nature of the unlawful activity and the clarity and specificity of the notification ([196]). In this respect, it should be observed that the mere provision of a NTD system may not be sufficient, per se, to ensure compliance with the requirement of expeditious removal, especially when the unlawful activity has the potential to cause serious harm. This is suggested by recent decisions of the European Court of Human Rights (ECHR) on the publication of defamatory content on news platforms ([197]). No guidance has yet been provided by the CJEU on the requirement of expeditious removal of the information.

2.3.3.4 Monitoring obligations

In accordance with Article 15(1) of the e-commerce Directive, ISSPs cannot have general obligations to monitor imposed upon them. Accordingly, injunctions imposed on ISSPs requiring them to install a filtering system that actively monitors all the data relating to all their service users, in order to prevent any future IP infringement, are not allowed ([198]). However, this does not preclude specific monitoring obligations ordered by courts or administrative authorities in the form of injunctions ([199]). Such specific

([195]) Bundesgerichtshof, 22 July 2010, Stokke/Tripp Trapp, I ZR 139/08, § 48.

([196]) Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016), § 12.144.

([197]) Delfi v Estonia, App. No. 64569/09, ECHR 16 June 2015 and Magyar Tartalomszolgáltatók v Hungary, App. No. 22947/13, ECHR, 2 February 2016. See Eleonora Rosati, 'The direct liability of intermediaries', in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020), p. 346.

([198]) 16/02/2012, C-360/10, SABAM, EU:C:2012:85, § 34-38; 24/11/2011, C-70/10, Scarlet Extended, EU:C:2011:771, § 47-54.

([199]) Recital 45 to e-commerce Directive. 03/10/2019, C-18/18, Glawischnig-Piesczek, EU:C:2019:821.

monitoring obligations are particularly relevant in the case of injunctions aimed at preventing future infringements.

The proposed DSA Regulation, while reaffirming the prohibition of general monitoring or active fact-finding obligations ([200]), specifies that 'voluntary own-initiative investigations' do not disqualify an intermediary service from the exemptions for mere conduit, caching or hosting ([201]).

2.3.4 Injunctions to prevent further infringements

Injunctions against intermediaries must be effective, proportionate, and dissuasive. They must neither create barriers to legitimate trade ([202]), nor impact on fundamental rights and freedoms ([203]). Therefore, an injunction that obliges ISSPs to take measures which could represent a significant cost for them, for example, cannot be permitted, as this can considerably impact on ISSPs' free use of the resources at their disposal ([204]).

The scope of injunctions against ISSPs includes both terminating existing infringements and preventing further infringements of that kind. In order to be effective, these injunctions require the implementation of some proactive monitoring duties, whose scope is limited by Article 15(1) ([205]). In the case of online marketplaces, these measures cannot comprise a duty to monitor all information submitted by their customers, or the banning of all sales of goods bearing a certain trade mark. The

([200]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 8.

([201]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 7.

([202]) 12/07/2011, C-324/09, L'Oréal SA-eBay, EU:C:2011:474, § 125-144.

([203]) 29/01/2008, C-275/06, Promusicae, EU:C:2008:54, § 61-70; 16/02/2012, C-360/10, *SABAM,* EU:C:2012:85, § 51-52.

([204]) 27/03/2014, C-314/12, UPC Telekabel Wien, EU:C:2014:192, § 45-50. See also Article 11 of Enforcement Directive.

([205]) See cases cited supra, note 198.

criterion for determining the scope of these kinds of injunctions can be derived from the 'double identity' approach suggested by Advocate General Jääskinen in the 'L'Oréal v eBay' case:

> [a]n appropriate limit for the scope of injunctions may be that of a double requirement of identity. This means that the infringing third party should be the same and that the trade mark infringed should be the same in the cases concerned. Hence, an injunction could be given against an intermediary to prevent the continuation or repetition of an infringement of a certain trade mark by a certain user. Such an injunction could be followed by an information society service provider by simply closing the client account of the user in question *([206])*.

This 'double identity' approach is not limited to trade mark infringement, as confirmed by the CJEU in a recent judgment concerning the removal of defamatory content from a social media platform. In that case, the Court ruled that Article 15(1) of the e-commerce Directive does not preclude a national court from ordering a platform to remove content which is not only identical, but also 'equivalent' compared to the content that was declared illegal; this on condition that the equivalence can be established without requiring the ISSP to carry out an independent assessment of the that content ([207]).

The CJEU jurisprudence suggests that injunctions to prevent further IP infringements are allowed, provided the service can comply with the order by using automated search tools. However, they cannot go as far as to require the service provider to carry out an independent assessment of the content.

([206]) Opinion of AG Jääskinen (12/07/2011, C-324/09, L'Oréal SA-eBay, EU:C:2010:757, § 182).

([207]) 03/10/2019, C-18/18, Glawischnig-Piesczek, EU:C:2019:821, § 53. On the relevance for trade mark infringement see Carina Gommers and Eva De Paw, 'Liability for trade mark infringement of online marketplaces in Europe: are they "caught in the middle"?', JIPL&P, 2020, Vol. 15, No. 4, p. 284.

2.3.5 Allocations of costs of injunctions

There are no harmonised rules on cost allocation of injunctions against intermediaries at EU level. As the UK Supreme Court highlighted in 'Cartier v British Telecommunications' ([208]), neither EU directives nor CJEU judgments offer specific guidelines as to the cost allocation of injunctions against intermediaries ([209]). Therefore, cost allocation is at the discretion of Member States ([210]). For example, a general rule in the UK was that intermediaries bear the costs of implementation, whilst rights holders pay the costs of application ([211]). However, in 'Cartier v British Telecommunications' ([212]), the UK Supreme Court set a new guideline for cost allocation by holding that 'unless there are good reasons for a different order an innocent intermediary is **entitled to be indemnified** by the rights-holder against the costs of complying with a website-blocking order' [emphasis added] ([213]).

([208]) [2018] UKSC 28.

([209]) Eleonora Rosati, 'UK Supreme Court holds that intermediaries have to bear no costs of injunctions against them' JIPL&P, 2018, Vol. 13, p. 933.

([210]) Eleonora Rosati, 'UK Supreme Court holds that intermediaries have to bear no costs of injunctions against them' JIPL&P, 2018, Vol. 13, p. 933.

([211]) Twentieth Century Fox and others v British Telecommunications PLC (*Newzbin 2*) [2011] EWHC 1981 (Ch).

([212]) [2018] UKSC 28.

([213]) [2018] UKSC 28, [31].

2.4 JURISDICTION OF IP INFRINGEMENT CASES

Key Points

Point 1

In settling conflicts of law in IP cases, national IP rights are governed by the Brussels I Regulation (recast) (*lex generalis*), whereas pan-EU IP rights, such as Community design rights or EU trade marks, are regulated by the relevant EU regulations (*lex specialis*).

Point 2

Claimants are generally obliged to bring a case to the courts where the defendant(s) is domiciled, but it is also possible to start proceedings, alternatively, in the place where the damage or the event that caused the damage to arise occurred, or where the infringement has been committed.

Point 3

In relation to allocation of jurisdiction in online infringement, one of the key factors to consider is whether infringers targeted either the EU (in case of pan-EU IP rights) or a Member State (in case of national IP rights). If the targeting requirement is established, IP rights holders may start proceedings in the courts of the targeted jurisdiction.

Point 4

Recognition and enforcement of foreign judgments between EU Member States is uniformly provided by the Brussels I Regulation (recast), while enforcing judgments in jurisdictions other than EU Member States can be extremely challenging, due to discrepancies in the national laws.

Over the last few decades the European Union (EU) has fought against IP rights infringement, with two clear goals: the first is to seek to combat IP rights infringement within the internal market and at the EU's external borders, and the second is to pre-empt IP theft taking place at the source, such as in third countries ([214]). In order to strengthen the EU IP regime for tackling IP rights infringement, the EU has introduced a number of Regulations and Directives, such as the Border Measures Regulation ([215]) and the Enforcement Directive ([216]) offering legal grounds for the enforcement of IP

([214]) Olivier Vrins and Marius Schneider, 'Cross-border enforcement of intellectual property: The European Union' in Paul Torremans (ed.), *Research Handbook on Cross-border Enforcement of Intellectual Property* (Edward Elgar 2014) 174.

([215]) Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003 [2013] OJ L181/15.

([216]) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L195/16.

rights and remedies, in relation to physical goods produced within the internal market or imported into the EU ([217]). Meanwhile, the Brussels I Regulation (recast) ([218]) was amended various times to improve access to justice in the EU Member States.

EU goals fighting against IP rights infringement:

- Goal 1: Seek to combat IPR infringement within the internal market
- Goal 2: Pre-empt IP theft taking place at the source, such as in third countries

The aim of this section is to provide an overview of the law on jurisdiction and conflicts of law in relation to IP rights infringement that take place in connection with the sale of infringing goods on online marketplaces. The Brussels I Regulation (recast) sets out general rules governing conflict of jurisdiction in civil and commercial matters, unifying differences between national rules in the Member States ([219]). In terms of settling conflicts of jurisdiction, the Brussels I Regulation (recast) directly applies to, and binds, the EU Member States, taking priority over national laws. However, the Regulation has limited effects on disputes regarding pan-EU IP rights, such as Community design rights or EU trade marks. This is because the specific rules on international jurisdiction for those rights are provided in the relevant regulations and take precedence over the Brussels I Regulation (recast) ([220]). In effect, the latter will generally apply in settling conflicts of jurisdiction in disputes

([217]) See Olivier Vrins and Marius Schneider, 'Cross-border enforcement of intellectual property: The European Union' in Paul Torremans (ed), *Research Handbook on Cross-border Enforcement of Intellectual Property* (Edward Elgar 2014) 182-195. See also European Commission Staff Working Document, 'Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States' (SEC(2010) 1589-final).

([218]) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) OJ L351/1.

([219]) Recital 4 to the Brussels I Regulation (recast).

([220]) Regulation (EU) No 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark [2017] OJ L154/1 (EUTMR), Article 125 and Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs [2002] OJ L3/1 (CDR), Article 82. To avoid confusion, it should be noted that the term 'international jurisdiction' adopted in the EUTMR and the CDR indicates 'pan-EU jurisdiction'. See David Stone, *European Union Design Law: A Practitioner's Guide,* 2nd edition (Oxford University Press 2016) § 22.56-22.95.

concerning **national IP rights**, whereas a matter of international jurisdiction in **EU IP rights** will be governed by the relevant regulations ([221]).

IP RIGHTS	LEGAL BASIS TO ESTABLISH JURISDICTION IN INTERNATIONAL (PAN-EU) IP DISPUTES
EU Trade Marks	EUTM Regulation No 2017/1001, Article 125
Community designs	Community Designs Regulation No 6/2002, Article 82
National IP rights (national trade marks, copyright and related rights, patents, …)	Brussels I Regulation (recast)

The provisions laid down by EU legislation only apply to civil proceedings. The rules to determine jurisdiction on criminal proceedings are not harmonised under EU law, and are left to the legislation of Member States and international law ([222]).

This section addresses pan-EU jurisdiction issues arising in relation to online infringement of national and EU IP rights, as well as disputes with non-EU undertakings, and recognition of foreign judgments. Finally, it briefly addresses jurisdiction issues in criminal proceedings.

([221]) Olivier Vrins and Marius Schneider, 'Cross-border enforcement of intellectual property: The European Union' in Paul Torremans (ed), *Research Handbook on Cross-border Enforcement of Intellectual Property* (Edward Elgar 2014) 206-11; 05/09/2019, C-172/18, AMS Neve and others, EU:C:2019:674, § 36.

([222]) EUIPO (2018) Study on legislative measures related to online IPR infringements, September 2018, and EUIPO (2021) International Judicial Cooperation in Intellectual Property Cases – Study on Legislative Measures Related to Online IPR Infringements Phase 2, March 2021.

2.4.1 Conflict of law in online infringement of national trade marks

The Brussels I Regulation (recast) states that, as a general rule, persons domiciled in a Member State will, whatever their nationality, be sued in the courts of that Member State ([223]). Article 63 of the Brussels I Regulation (recast) enlarges upon the meaning of being domiciled: a company or other legal person or association of natural or legal persons is domiciled at the place where it has its statutory seat, central administration or principal place of business, whereas determination of an individuals' domicile will be in accordance with national laws ([224]).

However, a person domiciled in a Member State may be sued in another Member State in exceptional situations ([225]). Article 7(2) of the Brussels I Regulation (recast) states that in matters relating to tort, delict or quasi-delict, a person may be sued in the courts of the place where the harmful event occurred or may occur. In other words, IP infringement cases can be heard in the courts where the harmful event occurred or may occur due to the infringement ([226]).

In 'Wintersteiger v Products 4U' ([227]), the CJEU clarified the meaning of Article 5(3) of the Brussels I Regulation, which is now Article 7(2) of the Brussels I Regulation (recast). The claimant, Wintersteiger, was an undertaking that was established in Austria and manufactured and sold winter sports equipment such as ski and snowboard servicing tools. The defendant, Products 4U, was a company that was established in Germany, and also developed and sold ski and snowboard tools. The defendant reserved the keyword 'Wintersteiger' on Google.de, so that when internet users entered the keyword into the search engine they were directed to the defendant's website. The claimant brought an action for infringement of an Austrian trade mark in the Austrian courts but the defendant contested the international jurisdiction of the Austrian courts, contending that Google.de and the advertisement that appeared on that website exclusively targeted German users.

([223]) Brussels I Regulation (recast), Article 4(1).

([224]) Brussels I Regulation (recast), Article 62. See also David Stone, David Stone, *European Union Design Law: A Practitioner's Guide* (2nd ed., Oxford University Press 2016) § 22.66.

([225]) Brussels I Regulation (recast), Article 7.

([226]) Paul Torremans, 'Jurisdiction in intellectual property cases' in Paul Torremans (ed), *Research Handbook on Cross-border Enforcement of Intellectual Property* (Edward Elgar 2014) p. 383.

([227]) 19/04/2012, C-523/10, Wintersteiger, EU:C:2012:220.

The CJEU held that the place where the harmful event occurred or may occur within Article 5(3) of the Brussels I Regulation (now Article 7(2)) meant both the place where the damage occurred and the place of the event giving rise to it, and that the defendant could be sued in either of those places ([228]). However, national IP rights are limited by their territoriality. Therefore, proprietors of the IP rights cannot generally rely on protection outside their jurisdiction ([229]). The CJEU held, therefore, that the court of the Member State in which the IP rights are registered (in this case, an Austrian trade mark) may have the power to assess and determine the case in the most effective manner ([230]). As for the place of the event giving rise to the damage, the CJEU pointed out that in the context of online advertising, the event should be construed as arising where the advertiser is using the referencing system for its own commercial communications, rather than the place of the servers providing the display of advertisements ([231]).

2.4.2 Conflict of law in online infringement of EU trade marks

More recently, an issue of jurisdiction in the context of online trade mark infringement was dealt with in 'AMS Neve v Heritage Audio' ([232]). The claimant (AMS Neve) was a company that was established in the UK and manufactured and sold audio equipment. The defendant (Heritage Audio) was a company that was established in Spain and sold and supplied audio equipment. The defendant was alleged to have offered for sale counterfeit goods bearing a sign that was identical or similar to the claimant's EU and national trade marks, to consumers in the UK via the defendant's website and

([228]) 19/04/2012, C-523/10, Wintersteiger, EU:C:2012:220, § 17-20.

([229]) 19/04/2012, C-523/10, Wintersteiger, EU:C:2012:220, § 25. Similarly, in Argos Ltd v Argos Systems Inc [2018] EWCA Civ 2211; [2019] FSR3, the Court of Appeal (UK) held that those who conduct their business entirely outside the UK jurisdiction should not be subject to UK trade mark law on the simple facts that UK residents can visit their website especially where such visit is not intended by the trader. See Mark Hyland and Michael Howard, 'The doctrine of targeting in the context of international trade mark disputes' (2019) *41 European Intellectual Property Review* 464.

([230]) 19/04/2012, C-523/10, Wintersteiger, EU:C:2012:220, § 28-29.

([231]) 19/04/2012, C-523/10, Wintersteiger, EU:C:2012:220, § 30-38.

([232]) 05/09/2019, C-172/18, AMS Neve and others, EU:C:2019:674. For a succinct analysis of jurisdiction issues of trade mark in the EU, see also 'International Jurisdiction in IPR Disputes' (European IP helpdesk) http://www.iprhelpdesk.eu/blog/international-jurisdiction-ipr-disputes, accessed 29 October 2020.

social media accounts, such as Facebook and Twitter ([233]). For this ground, the claimant brought an action for infringement to the Intellectual Property and Enterprise Court (IPEC) in the UK. However, the defendant contended that the UK courts had no jurisdiction to hear the case.

As mentioned above, in the case of EU trade mark infringement, rules on international jurisdiction in the relevant EU regulations take precedence over the Brussels I Regulation (recast), where the disputes arise internationally. In this case, the applicable provision was Article 97 of the Council Regulation (EC) No 207/2009, which is reproduced in Article 125 of the EUTMR. Article 97(1) of the Council Regulation (EC) No 207/2009 states that actions for infringement should be brought in the courts of the Member State in which the defendant is domiciled or, if not domiciled in any of the Member States, in which they have an establishment ([234]). Alternatively, pursuant to Article 97(5), it is also possible that infringement actions may be brought before the courts of the Member State in which the act of infringement has been committed or threatened ([235]).

Having referred to Article 97 of the Council Regulation (EC) No 207/2009, the IPEC concluded that the court had no jurisdiction over EU trade mark infringement cases because, pursuant to Article 97(1) of the Regulation, the Kingdom of Spain was the Member State in which the defendant was domiciled ([236]). Regarding the place where the act of infringement had been committed, the IPEC held that jurisdiction lay in the court of the Member State where the third party had decided to place the relevant advert, or to offer for sale products on the relevant site or platforms, and took steps to give effect to that decision ([237]). The claimant brought an appeal to the Court of Appeal (England & Wales) which sought a preliminary ruling on the interpretation of Article 97(5) of the Regulation.

Referring to the established case-law (e.g. that in 'Coty Germany' ([238])), the CJEU held that Article 93(5) of the Regulation relates to active conduct on the part of the person causing the alleged

([233]) 05/09/2019, C-172/18, AMS Neve and others, EU:C:2019:674, § 19-21.

([234]) Article 125(1) EUTMR provides the same rule.

([235]) Article 125(5) EUTMR.

([236]) 05/09/2019, C-172/18, AMS Neve and others, EU:C:2019:674, § 26.

([237]) 05/09/2019, C-172/18, AMS Neve and others, EU:C:2019:674, § 27.

([238]) 05/06/2014, C-360/12, Perfume bottle/Perfum bottle (3D), EU:C:2014:1318, which concerns issues of international jurisdiction in the context of offline EU trade mark infringement.

infringement ([239]). It went on to say that where the alleged infringement consisted of advertising and offering for sale counterfeit products, the place in which the infringement was committed was the territory where the consumers or traders targeted by those adverts or offers for sale, irrespective of whether the defendant was established elsewhere; whether the server of the electronic network that the defendant used was located elsewhere; or whether the products that were the subject of the adverts and offers for sale were located elsewhere ([240]).

2.4.3 Conflict of law in online infringement of copyright and related rights

Jurisdiction in online copyright infringement was first addressed by the CJEU in 'Pinckney v KDG Mediatech'. The dispute concerned the unauthorised reproduction on compact disc (CD) by an Austrian company of 12 songs, recorded by their French author on vinyl, and the sale of those CDs on the internet. The defendant challenged the jurisdiction of the French court on the ground that the CDs had been pressed in Austria at the request of a UK company, which marketed them on the internet. In response to the questions of the French Court of cassation, the CJEU clarified that the fact that the internet site where the allegedly infringing product was sold was accessible from a Member State, was sufficient to establish jurisdiction in that Member State, although the court only had jurisdiction to determine the damage caused in the Member State in which it was situated ([241]).

The 'accessibility approach' to the jurisdiction issue was then confirmed in 'Hejduk v EnergieAgentur' ([242]), a case on the unauthorised offering of photographs, taken by an Austrian professional photographer, on the website of a German company. The defendant raised the objection that the Austrian court lacked jurisdiction, since the website operated under a country-specific, German top-level domain and targeted a German public. The mere fact that it was 'accessible' from

([239]) 05/09/2019, C-172/18, AMS Neve and others, EU:C:2019:674, § 44. For a critical review of the case, see Eleonora Rosati, 'International jurisdiction in online EU trade mark infringement cases: where is the place of infringement located?' (2016) *38 European Intellectual Property Review* 482.

([240]) 05/09/2019, C-172/18, AMS Neve and others, EU:C:2019:674, § 47.

([241]) 03/10/2013, C-170/12, Pinckney, EU:C:2013:635.

([242]) 22/01/2015, C-441/13, Hejduk, EU:C:2015:28. In both this case and 03/10/2013, C-170/12, Pinckney, EU:C:2013:635, the jurisdiction issue was decided under Regulation (EC) No 44/2001, now repealed by Brusslels I Regulation (recast).

Austria was insufficient to confer jurisdiction to that court. However, the CJEU rejected that argument and clarified that 'accessibility' of a website in a Member State was sufficient to establish jurisdiction, subject to the limitation that the national court had jurisdiction only to rule on the damages caused in that Member State.

In a case of infringement of the *sui generis* database right, however, the CJEU ruled that the localisation of an act of reutilisation requires something more than just 'accessibility' in a given territory of the website containing the data extracted from the database. This is because due account must be taken of the 'ubiquitous nature' of internet websites, which can be consulted instantly everywhere by everyone 'irrespective of any intention of the operator of the website' and 'outside of [their] control' ([243]). Therefore, to establish that the infringing act occurs in a Member State, at least an 'intention' to target the public in that Member State must be shown. However, jurisdiction cannot be refused on the ground that the servers are located in a different place, as this would undermine the effectiveness of the protection given to databases under EU law ([244]).

2.4.4 Conflict of law in online infringement of Community designs

Jurisdiction in cases of infringement of Community designs was addressed by the CJEU in 'Nintendo/BigBen' ([245]). The Court clarified that, in a case with multiple defendants, when infringement proceedings are brought against a defendant domiciled in a Member State, the court also has jurisdiction over all the other co-defendants for infringing acts committed on the territory of other Member States. In particular, where a vendor is sued for infringement of a Community design in a Member State, and the manufacturer is based in another Member State, the national court has jurisdiction in relation to both of them. Moreover, where a design is reproduced and offered for sale on a website, the place where 'the process of putting the offer for sale online […] was activated' ([246]) is to be considered the place where the event giving rise to the damage occurred. Where the damage

([243]) 18/10/2012, C-173/11, Football Dataco and Others, EU:C:2012:642, § 35.

([244]) 18/10/2012, C-173/11, Football Dataco and Others, EU:C:2012:642.

([245]) 27/09/2017, C-24/16 & C-25/16, Nintendo, EU:C:2017:724.

([246]) 27/09/2017, C-24/16 & C-25/16, Nintendo, EU:C:2017:724, § 108.

has occurred in multiple jurisdictions, an overall assessment of the defendant's conduct should be made, rather than referring to each individual act of infringement.

2.4.5 International disputes with undertakings domiciled in non-EU Member States

In France, the claimant (Louis Vuitton), a French company, started proceedings against the defendants (eBay), an American company and a Swiss company, for trade mark infringement ([247]). The defendants used keywords included in some of the claimant's trade marks to generate adverts that directed internet users to their websites (e.g. ebay.fr and ebay.com). The defendants appealed the case, contending that the French courts had no jurisdiction, but American and Swiss courts did.

The French Supreme Court dismissed the appeal by holding that the French internet users were solicited by contentious keywords leading to offers of leather goods on various eBay auction sites managed by the eBay companies concerned ([248]). In support of its decision, the French Supreme Court highlighted, in particular, that:

(1) an eBay platform to which the internet user was directed offered leather goods in French, with a price in Euros or converted into Euros;
(2) the advertisements came from various vendors undertaking to deliver the goods in France and that these auction sites were managed by the eBay companies involved ([249]).

However, it was held that the UK courts had no jurisdiction in the case between a UK-based company (easyGroup, the owner of a brand of budget airline 'easyJet') and a company based in Bangladesh (EasyFly Express, a company providing airline cargo services), despite the defendant's allegedly infringing use of the claimant's trade marks ([250]).

([247]) Louis Vuitton Malletier (Société) v eBay Inc and eBay International AG [2011] I.L.Pr. 16 (Cour de Cassation).
([248]) Louis Vuitton Malletier (Société) v eBay Inc and eBay International AG [2011] I.L.Pr. 16 (Cour de Cassation), § 11.
([249]) Louis Vuitton Malletier (Société) v eBay Inc and eBbay International AG [2011] I.L.Pr. 16 (Cour de Cassation), § 11.
([250]) Mark Hyland and Michael Howard, 'The doctrine of targeting in the context of international trade mark disputes' (2019) *41 European Intellectual Property Review*, 464.

The defendant (EasyFly Express) put their 'EasyFly' logo onto their airplanes, and displayed it on their website. This logo used a typeface, colours and design that were markedly similar to the 'easyJet' trade mark. The claimant (easyGroup) brought an action to the High Court (England and Wales) for infringement of UK and EU registered trade marks ([251]). Arnold J, applying the principles on international jurisdictions established in 'AK Investment CJSC v Kyrgyz Mobile Tel Ltd' ([252]) to this case, held that in order for use of a sign to qualify as use in the UK or elsewhere in the EU – and therefore amount to trade mark infringement – the use must target the UK or elsewhere in the EU ([253]). Upon considering the factual evidence, Arnold J held that the claimant did not have a real prospect of establishing that the defendant has targeted the UK or the EU.

In particular, according to Arnold J, the mere fact that the defendant's website and Facebook page were in English would not directly lead to the assumption that the website and webpage target the UK. This is because English is widely spoken in Bangladesh in business contexts, as well as globally ([254]). Furthermore, online advertising on the defendant's website using statements such as 'our network provides a global reach for customers in Africa, Europe, North America, South America, the Middle East, South East Asia and North Asia' would also not directly lead to the assumption that the defendant was targeting Europe, especially where such statements were likely to be perceived by average consumers as advertising hype ([255]).

([251]) Easygroup Ltd v Easy Fly Express Ltd [2018] EWHC 3155 (Ch), § 5-6.

([252]) [2011] UKPC 7; [2012] 1 WLR 1804, § 71, 81, § 88 (summarised by Arnold J: First, the claimant must satisfy the court that, in relation to the foreign defendant to be served with the proceedings, there is a serious issue to be tried on the merits of the claim, i.e. a substantial question of fact or law or both. Second, the claimant must satisfy the court that there is a good arguable case that the claim against the foreign defendant falls within one or more of the classes of case for which leave to serve out of the jurisdiction may be given (often referred to as 'the gateways') which are set out in paragraph 3.1 of Practice Direction 6B. Lastly, the claimant must satisfy the court that in all the circumstances England is clearly or distinctly the appropriate forum for the trial of the dispute and that in all the circumstances the court ought to exercise its discretion to permit service of the proceedings out of the jurisdiction.).

([253]) Easygroup Ltd v Easy Fly Express Ltd [2018] EWHC 3155 (Ch), § 10.

([254]) Easygroup Ltd v Easy Fly Express Ltd [2018] EWHC 3155 (Ch), § 18.

([255]) Easygroup Ltd v Easy Fly Express Ltd [2018] EWHC 3155 (Ch), § 20-21.

2.4.6 Recognition and enforcement of foreign judgments

So far, this section has discussed the law on jurisdiction in international IP disputes. According to the key cases discussed above, it was established that IP rights holders may initiate proceedings not only in the national courts in the place where the defendant is domiciled, but also in the national courts where the claimant is based. However, this is on the condition that it is deemed to be the place where damage occurred or the infringement was committed.

However, owing to the separation of national judicial systems, the effects of a judgment are, in principle, confined within the territorial boundaries of the country where the court that delivered the judgment is located ([256]). As a corollary, the convenience for the rights holders provided by the ability to start lawsuits and obtain judgments against foreign defendants in their home country may be offset, or even futile, without the recognition and enforcement of those judgments in the country in which the foreign defendant is domiciled.

Therefore, uniform recognition and enforcement of judgments relating to IP rights may only be, available where there are legal grounds such as international agreements in place between the countries in which the claimant and defendant are domiciled – whether those be international, multilateral, or bilateral treaties, or regional agreements.

Currently at an international level there are no uniform international rules on the recognition and enforcement of judgments relating to IP rights. International frameworks for IP rights such as the Agreement of Trade-Related Aspects of Intellectual Property Rights (TRIPs) or the World Intellectual Property Organisation (WIPO) Treaties do not provide rules on cross-border recognition and enforcement of judgments ([257]).

([256]) Pedro A. De Miguel Asensio, 'Recognition and enforcement of judgments: Recent developments' in Paul Torremans (ed), *Research Handbook on Cross-border Enforcement of Intellectual Property* (Edward Elgar 2014), p. 469.

([257]) Pedro A. De Miguel Asensio, 'Recognition and enforcement of judgments: Recent developments' in Paul Torremans (ed), *Research Handbook on Cross-border Enforcement of Intellectual Property* (Edward Elgar 2014), p. 472.

At an EU level, both EUTMR and CDR lack provisions on recognition and enforcement of judgments in civil matters, as does the Enforcement Directive ([258]). On the other hand, Chapter III of the Brussels I Regulation (recast) ([259]) deals with recognition and enforcement of judgments by providing that, as a general rule, a judgment given in a Member State will be recognised ([260]) and enforceable ([261]) in the other Member States, without any special procedure being required. The effects of the Brussels I Regulation (recast) are, however, limited to EU Member States. Therefore, a judgment rendered in an EU Member State may or may not be recognised and enforced in non-EU countries, and the extent to which it is recognised and enforced will vary from country to country, depending on the content of the agreement, if any, between the countries and their national laws ([262]).

For example, there was a case where issues of recognition and enforcement of judgments arose between French design companies and an American news report company ([263]). Although it was related to copyright, this case proved that enforcement of judgments in other jurisdictions may well be contested by their national laws, leading to difficulty in pursuing foreign infringers ([264]).

Two French companies (Sarl Louis Feraud International and S.A. Pierre Balamain) dealing with high-fashion clothing and other items for women brought an action to the High Court of Paris (Tribunal de grande instance de Paris) for trade mark and copyright infringement against the defendant (Viewfinder, a US-based corporation with its main office in New York) ([265]). The defendant uploaded

([258]) Pedro A. De Miguel Asensio, 'Recognition and enforcement of judgments: Recent developments' in Paul Torremans (ed), *Research Handbook on Cross-border Enforcement of Intellectual Property* (Edward Elgar 2014), p. 474.

([259]) Articles 36-57 of the Brussels I Regulation (recast).

([260]) Article 36(1) of the Brussels I Regulation.

([261]) Article 39 of the Brussels I Regulation (however, the judgment given in a Member State is required to be enforceable in that country in the first place to be enforceable in the other Member States).

([262]) Pedro A. De Miguel Asensio, 'Recognition and enforcement of judgments: Recent developments' in Paul Torremans (ed), *Research Handbook on Cross-border Enforcement of Intellectual Property* (Edward Elgar 2014), p. 476.

([263]) Sarl Louis Feraud International v View finder, Inc., 489 F.3d 474 (2d Cir. 2007).

([264]) Marketa T Landova, 'The potential worldwide application of the US fair use defence' (2008) *30 European Intellectual Property Review*, p. 38.

([265]) Sarl Louis Feraud International v View finder, Inc., 489 F.3d 474 (2d Cir. 2007). For case comments, see Marketa T Landova, 'The potential worldwide application of the US fair use defence' (2008) *30 European Intellectual Property Review*, 38.

photographs of fashion shows held by designers around the world – including those of the claimants' fashion shows – to the website it operates. The High Court of Paris held that the act of uploading photographs of the claimants' fashion shows, without the necessary authorisation, amounted to counterfeiting and violation of royalties, pursuant to Articles L716-1 and L122-4 of the Intellectual Property Code.

Upon obtaining the judgment, the claimant filed separate complaints to the US District Court for the Southern District of New York to enforce the judgment, in accordance with New York's Uniform Foreign Money Judgment Recognition Act. This Act made it possible for foreign judgments (which are final, conclusive and enforceable in the country where there were rendered) to be recognised and enforced in New York ([266]).

The defendant disputed the enforceability of French judgments in the US, by contending that, inter alia, enforcing the French judgment would be repugnant to the public policy of New York, as it would violate the defendant's First Amendment rights ([267]). The District Court accepted the defendant's submission on the ground that the 'First Amendment simply does not permit plaintiffs to stage public events in which the general public has a considerable interest, and then control the way in which information about those events is disseminated in the mass media' ([268]).

In the appeal, the US Court of Appeals for the Second Circuit highlighted that the District Court had erred in applying First Amendment rights in this case, by holding that First Amendment rights coexist with copyright laws. Therefore, even though the defendant's ability to gather and report the news may have been incidentally restricted, the defendant was not permitted to use other's copyrighted works without complying with the copyright laws ([269]). It further noted that conflicts between interests protected by the First Amendment and the copyright laws could be resolved by application of the fair use doctrine. Applying the fair use doctrine, the Court of Appeals for the Second Circuit held that there

([266]) Sarl Louis Feraud International v View finder, Inc., 489 F.3d 474 (2d Cir. 2007), 477.

([267]) Sarl Louis Feraud International v View finder, Inc., 489 F.3d 474 (2d Cir. 2007), 478. (N.Y. C.P.L.R § 5304(b)(4) states that "a foreign country judgment need not be recognised if … the cause of action on which the judgment is based is repugnant to the public policy of this state").

([268]) Sarl Louis Feraud International v View finder, Inc., 489 F.3d 474 (2d Cir. 2007), 478.

([269]) Sarl Louis Feraud International v View finder, Inc., 489 F.3d 474 (2d Cir. 2007), 480-81.

was insufficient factual evidence presented and analysed by the District Court and decided to vacate the judgment of the District Court ([270]).

2.4.7 Criminal jurisdiction

Jurisdiction in criminal law matters is generally based on the principle of territoriality. Currently, there are no binding instruments under EU law to resolve conflicts of jurisdiction in criminal matters ([271]). In cases where EU law prescribes extraterritorial jurisdiction, thereby triggering potential conflict, the principle of *non bis in idem* (i.e. the right to not be prosecuted twice for the same offence), which is enshrined in primary EU law, applies ([272]).

An important instrument of international law that can be of assistance in determining adjudication in criminal proceedings against online IP infringers is the Council of Europe Cybercrime Convention 2001 ([273]). Jurisdiction is addressed in Article 22, which applies to all substantive crimes in the convention, including Article 11 'Offences related to infringements of copyright and related rights'. The offences covered by the provision include wilful copyright infringement on a commercial scale carried out by means of a computer system. The principles of adjudication laid down by the convention are:

i. ubiquity (territory of origin or territory of effect of the crime);
ii. nationality (offence committed by a national from outside the territory);
iii. legislative extraterritoriality (nationals are obliged to comply with domestic law, even when they are outside the territory); and
iv. representation (act carried out by a national and extradition is refused) ([274]).

([270]) Sarl Louis Feraud International v View finder, Inc., 489 F.3d 474 (2d Cir. 2007), 482-84.
([271]) European Law Institute (2017) Draft legislative proposals for the prevention and resolution of conflicts of jurisdiction in criminal matters in the European Union. p. 9.
([272]) EU Charter of Fundamental rights, Article 50.
([273]) Convention on Cybercrime, ETS No 185.
([274]) EUIPO (2021) International judicial cooperation in intellectual property cases (March 2021), p. 33.

Moreover, Article 25, which lays down general principles on mutual assistance, determines that, when assistance is sought for a criminal offence, the condition of 'dual criminality' is fulfilled irrespective of whether the laws of one of the countries place the offence in the same category or denominate the offence by the same terminology. This provision provides wide scope for adjudication in criminal cases related to online copyright infringement.

Conclusion

The misuse of online marketplaces and social media platforms to advertise, sell and distribute IP-infringing goods poses specific enforcement challenges to rights holders, intermediaries, and law enforcement agencies alike. The available measures to tackle IP infringements involve a range of both voluntary good practices developed in collaboration between rights holders and intermediaries, and legal instruments for law enforcement. The existing EU legal framework creates strong incentives for intermediaries to actively collaborate with rights holders and law enforcement agencies across the whole supply chain of IP-infringing goods. Online marketplaces have implemented and developed effective measures in the framework of the MoU signed in 2011, later revised in 2016 ([275]). These measures are aimed at preventing and repressing the misuse of their services by vendors of IP-infringing goods. However, infringers apply a number of techniques to elude detection, takedown, and the suspension of vendor accounts. Among the current and emerging trends, the following pose a particular challenge to enforcement efforts:

- **Opening multiple vendor accounts**. Infringers open multiple accounts under different names on the same platform and across different media to elude **repeat offender policies**. Under these policies, users that repeatedly violate the platform's T&C may have their accounts suspended or disabled.

([275]) European Commission, *Memorandum of understanding on the sale of counterfeit goods on the internet*, https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en.

- **Misuse of online advertising**. Vendors manipulate online advertising services by associating their illicit activity with famous brands, and by placing adverts aimed at directing traffic to external websites or to the listings of online marketplaces offering IP-infringing goods.

- **Misuse of social media functionalities.** Vendors misuse the functionalities of social media platforms to reach a high number of consumers ([276]). An emerging trend is the use of **live-streaming sales** to advertise IP-infringing goods. Vendors adopt various techniques to elude the platforms' enforcement measures; for instance, orders are received either via links and/or codes shared during the streaming or directly from the stream's live-chat. Therefore, once the stream is over, there is no evidence left to trace.

These trends call for enhanced cooperation in enforcement actions. At legislative level, some of the measures proposed in the **DSA Regulation** are clearly going in this direction. The proposal builds on the best practices adopted by online marketplaces in the framework of the MoU and introduces specific obligations for online platforms. These include, in particular, mandatory notice-and-action mechanisms ([277]), 'trusted flaggers' programmes ([278]), the suspension of repeated misusers ([279]) and the notification of suspected criminal offences to law enforcement agencies ([280]). Of particular relevance for the efficacy of enforcement actions against repeated offenders is the provision on **traceability of traders**, namely the obligation that online marketplaces obtain and verify the identity

([276]) EUIPO (2021) *Monitoring and analysing social media in relation to IP infringement*; EUIPO (2021) *Social Media – Discussion Paper. New and existing trends in using social media for IP infringement activities and good practices to address them*, June 2021.

([277]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 14 and 15.

([278]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 19.

([279]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 20.

([280]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 21.

of traders ([281]). As discussed above on this report ([282]), the traceability of traders is a powerful deterrent against the misuse of marketplaces by individuals holding multiple vendor accounts. In the same vein, the provision on **advertising transparency** will help repress the abuse of online advertising services of IP-infringing goods ([283]).

These provisions are part of a broader Commission's Action Plan to reinforce cooperation between all involved players to curb IP infringement. The IP Action Plan announced the establishment of an **EU toolbox against counterfeiting**, setting out principles for coordinated action, cooperation and data sharing among right holders, intermediaries and law enforcement authorities ([284]). The toolbox will also promote the use of new technologies such as image recognition and AI to tackle IP infringements.

The proposed actions reaffirm the commitment of the EU legislator to incentivise collaboration among all stakeholders involved in tackling illegal activities online. Rights holders and law enforcers in the EU have a range of judicial and extra-judicial instruments to counteract IP infringement that is occurring via vendor accounts on third-party trading platforms. Increased communication among rights holders, online platforms, and law enforcement agencies can improve the detection and removal of IP-infringing goods that are offered for sale, unknowingly, on the marketplace or advertised on social media. Follow-the-money investigations can provide the necessary evidence to initiate judicial proceedings against the vendor. Overall, a better understanding of the business models and the supply chain of IP-infringing goods can help determine where, when, and how to effectively apply those instruments.

([281]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 22.

([282]) section 2.1.1.2.

([283]) Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive No 2000/31/EC, COM/2020/825 final, Article 24.

([284]) Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recovery and resilience. Brussels, 25.11.2020. COM(2020) 760 final, p. 21.

APPENDIX: Case studies

The case studies reported in this Appendix are illustrative of the range of IP-infringing activities committed by vendors on third-party online marketplaces, as discussed in the report. The cases are analysed and presented according to the model canvas developed in Phase 1 – Research on Online Business Models Infringing Intellectual Property Rights ([285]). For the purpose of this study, a further dimension has been introduced, namely the category of infringing goods object of a transaction (as defined in subsection 1.2.1).

CASE	DESCRIPTION	INFRINGING GOODS	MARKETPLACES
1	Listings on marketplace for handcrafted items	Brand exploitation	Marketplace for independent retailers
2	Sale of digital artwork bearing a famous brand on marketplace for NFT	Brand exploitation	Marketplace for digital goods
3	Counterfeit medicines and drugs	Grey market	Stand-alone website with social media presence
4	Sale of clones of branded mobile phones	Confusion	Wholesale marketplace
5	Advertisement of counterfeit sale on live-streaming channel	Counterfeit (fakes)	Social media marketplace
6	Fake luxury goods sold as pre-owned items on auction marketplace	Counterfeit (fakes)	Marketplace for auctions and second-hand goods
7	Vendor of counterfeit perfumes on social media marketplaces	Counterfeit (fakes and replicas)	Social media marketplace
8	Vendor of counterfeit luxury brands on social media platform	Counterfeit (replicas)	Social media marketplace
9	Vendor on dark web marketplace	Counterfeit (replicas)	Dark web marketplace
10	Network of websites selling high quality replicas of luxury goods	Counterfeit (replicas)	Stand-alone website with social media presence
11	Sale of back-up copies of computer programs on marketplace for auctions	Pirated goods	Marketplace for auctions and second-hand goods
12	Sale of subscriptions to major online streaming services	Pirated goods	Stand-alone website with social media presence
13	Vendor of subscriptions to pay-TV and online streaming services	Pirated goods	Wholesale marketplace

([285]) EUIPO (2016) *Research on Online Business Models Infringing Intellectual Property Rights, Phase 1 – Establishing an overview of online business models infringing intellectual property rights*, July 2016.

CASE No 1	Vendor Accounts on Third Party Trading Platforms: Listings on marketplace for handcrafted items

Case study based on an investigation performed by the project team

Date of analysis: 17/02/2021 | Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary

Listing on a marketplace for handcrafted items. The marketplace enables artists to promote their designs and creations. Customers can buy phone cases, mugs, pins, and many other goods, with an artist's design printed on them. In this case, an artist sells a phone case with the logo of a popular sportswear brand.

Matrix		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C2	D2	E2	F2
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	**Products and Services**	**Involved IPR(s)**
Open internet. Marketplace for handcrafted items.	Brand exploitation: use of a sportswear brand's logo on handicraft items.	Trade marks, design.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Vendors located in France.	Direct sale to customers. Payment methods: PayPal and bank transfer (via Sofort). Shipping methods: UPS, FedEx, DHL.	Items were promoted through a Telegram group with approximately 3 500 members.

Resilience Against Enforcement Action	
The brand name is not mentioned in the title of the listing.	
Marketing Channels and Internet Traffic Features	
The marketplace hosting the shop.	
Customer Incentives	
Products with attractive designs and an artistic touch.	

CASE No 2	Vendor Accounts on Third Party Trading Platforms: Sale of digital artwork bearing a famous brand on marketplace for non-fungible tokens

Case study based on an investigation performed by the project team

Date of analysis: 06/04/2021 | Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary

Digital artwork produced by a digital artist was uploaded on a popular marketplace for non-fungible tokens (NFT). The artwork depicted a ghost branded with the logo of a famous luxury brand. The artist made 45 copies of this work available and sold all of them for USD 200 each. Some of the copies were on sale for as much as USD 180 000, and one had already been re-sold for GBP 13 000.

Matrix		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C2	D2	E2	F2
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	**Products and Services**	**Involved IPR(s)**
Open internet. NFT (non-fungible token) marketplace.	Brand exploitation: use of a famous luxury brand on NFT.	Trade marks.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Based on the leaks from their standalone website, the artist is most likely based in the USA.	Payment methods: Ethereum (ETH).	

Resilience Against Enforcement Action	
All information on the provenance and ownership of the item (including historical information of ownership transfers) is captured on a blockchain. This information is accurate and immutable but, at the same time, can depict an anonymous user, requiring further investigation.	
Marketing Channels and Internet Traffic Features	
The marketplace hosting the item as uploaded by the digital artist. The artist also maintains their own site selling physical goods using the Shopify platform.	
Customer Incentives	
Like all art items, ownership of digital art can be seen as an investment, as the customer can easily resell the digital item at a higher price.	

CASE No 3	Vendor Accounts on Third Party Trading Platforms: Counterfeit medicines and drugs

Case study based on an investigation performed by the project team

Date of analysis: 11/03/2021 | Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary

The investigation started from a suspicious subdirectory of a hospital's website in Ecuador. This revealed a network of websites selling medicines that had been imported illegally from foreign countries. The medicines were mainly sexual enhancers. Investigations led to a company registered in Cyprus connected with this case. It uses a custom-developed portal for payments which is used by websites linked to this case. There is a high probability of credit card fraud. They usually include logos claiming that they are certified by pharmacy associations.

Matrix		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C2	D2	E2	F2
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	Products and Services	Involved IPR(s)
Open internet. Website controlled by infringer.	Grey market products: pills, mainly sexual enhancers.	Patents, supplementary protection certificates, trade marks.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Vendors located in Russia and Ukraine. Company registered in Cyprus.	Direct sales to customer. Payment method: credit card only. Shipping options: EMS/airmail.	The pharmacy only allows payments made via major credit card vendors such as Visa, Mastercard, AMEX, Discover, Diners Club,

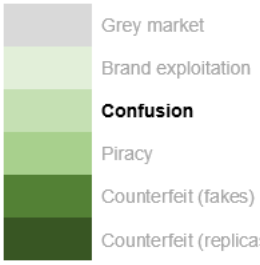
Resilience Against Enforcement Action	JCB, and e-checks. They do not support any other options. However, the pharmacy is using fake SSL certificates from reputed vendors, such as GeoTrust, SecurityMetrics, on their website instead of genuine ones. This suggests that a customer might fall victim to identity theft on the platform during checkout without prior knowledge. The website has some reviews from customers on its platform. However, some customers have noted that the reviews are either fake or they were purchased. The website cannot be trusted.
n/a	
Marketing Channels and Internet Traffic Features	
-	
Customer Incentives	
High-quality medical products, a professional customer service team that is always available to answer queries, generous bonuses and discounts, as well as a secure and reliable platform. All these claims are appealing to the customer.	

CASE No 4	Vendor Accounts on Third Party Trading Platforms: Sale of clones of branded mobile phones

Case study based on an investigation performed by the project team

Date of analysis: 13/03/2021 | Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



Manufacturer of smartphones, tablets and smart watches based in China. The company earned notoriety for releasing clones of popular high-end smartphones.

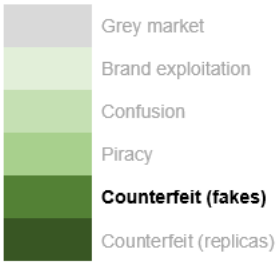
Matrix	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C2	D2	E2	F2
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	**Products and Services**	**Involved IPR(s)**
Open internet. Wholesale marketplaces.	Confusingly similar products: clones of popular high-end smartphones, smart watches and tablets.	Patents, design, trade marks.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Vendors and producers located in China.	Direct sale to customers or to resellers. There is no store with the name of the company. However, stores selling specifically these products and nothing else can be found. Therefore, we assume the revenue sources are both from direct sales and resellers.	Customers are aware that they are buying a clone of a high-end smartphone which is different from the original. Based on the feedback on vendors' accounts on a wholesale marketplace, buyers seem to be satisfied with the quality of the product.

	Payment methods: the vendors use payment systems made available by third party marketplaces. Delivery method: ePacket, TNT Express, DHL.	
Resilience Against Enforcement Action		
The brand logo is removed from the product images. The product looks different from what is presented in the listing.		
Marketing Channels and Internet Traffic Features		
Reviews videos on YouTube. There is an inactive Facebook page from 2013.		
Customer Incentives		
The company offers a product which is a close replica of the original in terms of design and user interface at a really low price.		

CASE No 5	Vendor Accounts on Third Party Trading Platforms: Advertisement of counterfeit sale on live-streaming channel
Case study provided by expert interviews	
Date of analysis: 23/11/2020	Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



Sale of counterfeit luxury bags.

The product is advertised in the course of a live stream sale on a major social media site. During the live stream, the speaker provides a code and a link to a listing published on an online marketplace. The listing does not refer to the product and is apparently unrelated to infringing products. By including the code in the order and completing the payment, the user receives the product advertised in the live stream.

The business comprises a livestream facility with 8 rooms and 30-40 employers working 24/7. Every room is designed with backdrop shelves and streaming equipment.

Matrix	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C2	D2	E2	F2
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	**Products and Services**	**Involved IPR(s)**
Open internet. Marketplace livestream sales.	Fake products: luxury bags.	Trade marks.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Vendors located in China.	Payment is made through known online marketplaces.	Counterfeiters work continuously, in three 8-hours shifts, as they are advertising 24/7.

Resilience Against Enforcement Action		
The infringers avoid any reference to trade marks in the live stream and in the listings, in order to elude detection. The transaction is made on a product page that is completely unrelated to the counterfeit product.		
Marketing Channels and Internet Traffic Features		
Live streaming sales.		
Customer Incentives		
Customers in this specific example know that they are buying counterfeit products as they pay for some other product and expect the product that was advertised on live stream.		

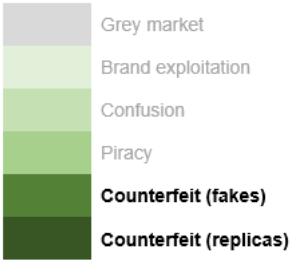
CASE No 6	Vendor Accounts on Third Party Trading Platforms: Fake luxury goods sold as pre-owned items on auction marketplace

Case study based on an investigation performed by the project team

Date of analysis: 07/03/2021

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



Profile on auction marketplace selling pre-owned luxury items mainly through auctions. There is suspicious user feedback indicating that counterfeit products are being sold among original ones. The target has been operating for 9 years on the platform and has sold more than 15 000 items.

Matrix		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C2	D2	E2	F2
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	**Products and Services**	**Involved IPR(s)**
Open internet. Auction marketplace.	Fakes and replicas sold as pre-owned products, mainly bags and wallets.	Trade marks.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Vendor located in Japan.	Direct sale to customers. Payment method: PayPal only. Shipping methods: EMS, ePacket, DHL.	There is negative feedback from a buyer claiming that their bag came with a non-existent serial number. Another customer claimed that the product they received was a fake.
Resilience Against Enforcement Action		
n/a		

Marketing Channels and Internet Traffic Features	
Twitter account with zero activity.	
Customer Incentives	
The profile has a great many positive reviews and has been operating for many years, offering more than 900 different items at the time of writing.	

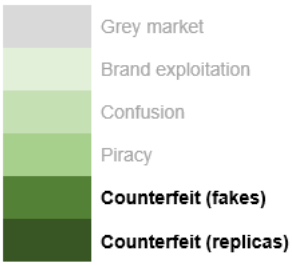
CASE No 7	Vendor Accounts on Third Party Trading Platforms: Vendor of counterfeit perfumes on social media marketplaces

Case study extracted from a news article

Date of analysis: 20/02/2021

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



The sales and live streams of fake perfumes took place at a shop in Turkey. The Turkish Police raided the vendors after seeing a notice during an online streaming session on a major social media platform and caught the infringers at the very moment they were streaming.

Counterfeit perfumes and other fake goods (smart watches) were advertised through live streaming on social media websites.

Matrix		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D2	E2	F2
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology

Open internet.

Social media marketplaces and live streaming sales.

Products and Services

Fakes and replicas sold as original products: perfumes and wrist watches.

Involved IPR(s)

Trade marks.

Identification of Infringer

Vendors located in Turkey.

Revenue Sources

Direct sale to consumers at physical shop and on social media marketplaces.

Customer Relations

Through social media accounts and online marketplaces.

Resilience Against Enforcement Action

n/a

Marketing Channels and Internet Traffic Features	
A shop in Turkey and social media presence.	
Customer Incentives	
Products are advertised as genuine and the sale takes place in an actual shop. Hence customers are tricked into believing that they are buying ‘bargain’ genuine products.	

CASE No 8	Vendor Accounts on Third Party Trading Platforms: Vendors of counterfeit luxury brands on social media platforms

Case study based on an investigation performed by the project team

Date of analysis: 12/03/2021

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary

This is a large network of counterfeit vendors operating on various social media marketplaces. The main marketplace is on Facebook, with over 10 000 users. There are also two Telegram groups. One for DHgate listings and another one for AliExpress. There is a blog in Teletype with detailed information related to high quality counterfeit products. Many of the products listed on the Telegram groups are showcased on the Yupoo platform.

Matrix	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C2	D2	E2	F2
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	Products and Services	Involved IPR(s)
Open internet. Wholesale marketplaces and social media.	Replicas: watches, clothing and bags. Luxury brands.	Trade marks.

Identification of Infringer	Revenue Sources	Customer Relations
Network of vendors located in China.	Direct sale to customers. Payment methods: the vendors use payment systems made available by third party marketplaces. Delivery method: ePacket.	Customers are provided with detailed instructions related to the ordering process. Each product has a unique ID which the customer must mention in the ordering steps as a message to the seller. Customers are also advised to avoid mentioning the real product or the brand.

Resilience Against Enforcement Action	There are numerous reviews and comments regarding the delivery and the quality of the products in the Facebook group. There are a few customers who had trouble with customs and other members provided them with advice on how to deal with the situation. Screenshots with the shipping path can also be found.
Listings on marketplaces do not mention brand names and appear to sell a different product, often just a white T-shirt.	
Marketing Channels and Internet Traffic Features	
Private Facebook groups, Telegram group, Teletype blog.	
Customer Incentives	
Luxury goods of extremely high quality at low prices.	

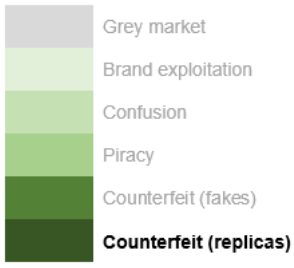
CASE No 9	Vendor Accounts on Third Party Trading Platforms: Vendor on dark web marketplace

Case study based on an investigation performed by the project team

Date of analysis: 02/02/2021

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



Vendor on Versus. Versus is a marketplace operating on the dark web. Like most dark web marketplaces, they attempt to moderate and arbitrate the transaction between the vendor and the buyer, through the use of escrow accounts. This particular vendor sold over 200 items through this platform in the past year. They advertised a 'high-end replica' of famous brand T-shirt and claimed to ship it from Hong Kong. The vendor received high ranks, making them a popular vendor. However, the marketplace itself was accused of exit scam behaviour, affecting the hosted vendors, some of which were looking to move their businesses to other marketplaces.

Matrix	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C2	D2	E2	F2
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	Products and Services	Involved IPR(s)
Dark web. Versus.	Replicas: famous brand T-shirts.	Trade marks.

Identification of Infringer	Revenue Sources	Customer Relations
Unknown vendor, shipping goods from Hong Kong.	Direct sale to customers by cryptocurrency (escrow wallet).	The vendor does not hide the fact that their product is counterfeit; they make the case of being a high-quality counterfeit (AAA) as the transaction is only completed upon the

Resilience Against Enforcement Action	customer receiving and confirming that they are happy with the product. Reputation is of utmost importance in the dark web. In many cases the vendor posts their own photos of the product to prove possession.
Use of IP address anonymisation (The Onion Routing protocol) to hide the location of the marketplace. The vendor uses PGP to encrypt direct communication with them.	
Marketing Channels and Internet Traffic Features	
Listing directly on the dark web marketplace.	
Customer Incentives	
Low price, customer is aware that the product is counterfeit and they can trigger remedial actions if the product is not as expected or advertised (in terms of replica quality).	

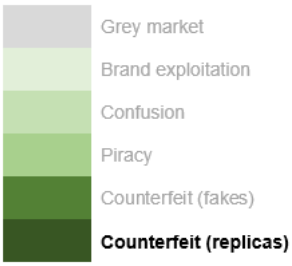
CASE No 10	Vendor Accounts on Third Party Trading Platforms: Network of websites selling high quality replicas of luxury goods

Case study based on an investigation performed by the project team

Date of analysis: 17/02/2021

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



This business model involves a network of websites selling counterfeit goods of high quality. Most of the domains use the '.ru' top-level domain and contain the same products. However, the websites have different domain names. Online personas are also used for promotion through social media platforms. Each website has its influencers with their contact information. Many of the websites contain links to YouTube channels where products are being presented and reviewed. Another strategy is to send products to YouTubers with low-medium reach for free. Content creators publish a detailed review and promote the corresponding website.

Matrix		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C2	D2	E2	F2
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	**Products and Services**	**Involved IPR(s)**
Open internet. Independent group of websites.	Replicas: watches, sneakers, bags, clothes, belts, socks, etc.	Trade marks.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Networks of vendors located in China.	Payment methods: PayPal, Western Union, Cash App. Shipping methods: UPS, FedEx, DHL.	The websites come with a blog containing instructions on how to order a product, and articles regarding the latest trends and

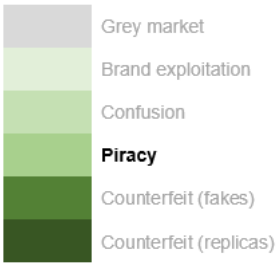
<table>
<tr><td>Resilience Against Enforcement Action</td><td rowspan="4">releases. There are a lot of Instagram profiles posing as employees of the shop. Potential customers can contact them on WhatsApp or view customer reviews under the highlights section of their profile. The marketing strategy through content creators seems to work even better as the reach is maximal, with minimal exposure of the supplier.</td></tr>
<tr><td>The brand name is not mentioned in the title of the listing. Another strategy against enforcement is to keep the nominal prices high enough to avoid detection from automated systems.</td></tr>
<tr><td>Marketing Channels and Internet Traffic Features</td></tr>
<tr><td>The marketplace hosting the shop, presence on major social media platforms and instant messaging groups.</td></tr>
<tr><td colspan="2">Customer Incentives</td></tr>
<tr><td colspan="2">Prices are low but still expensive giving the impression that the products are ‘good bargain’ originals. There are thousands of videos on YouTube related to this business, creating a sense of security and reliability.</td></tr>
</table>

CASE No 11	Vendor Accounts on Third Party Trading Platforms: Sale of back-up copies of computer programs on marketplace for auctions

Case study based on Latvian Courts' civil and criminal proceedings leading to the final ruling of the Court of Appeal on 26 September 2017 and involving a referral to the CJEU for preliminary ruling (12/10/2016, C-166/15, Ranks and Vasiļevičs, EU:C:2016:762).

Date of analysis: 12/03/2021 | Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



Two Latvian citizens engaged in selling CDs with back-up copies of various editions of Microsoft Windows and Office software on eBay. The vendors registered on eBay as natural persons, frequently changing their user name. Initially, they operated from the USA, but then they moved to Germany and Latvia, from where they shipped to different countries. They used their private eBay account to purchase licensed Microsoft software. Some of the copies were sold with a Microsoft certificate of authenticity, that the vendors bought separately and attached to the copies in order to demonstrate their authenticity.

Matrix	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C2	D2	E2	F2
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	Products and Services	Involved IPR(s)
Open internet. Marketplace for auctions (eBay).	Pirated goods: back-up copies of Microsoft software and activation codes of Microsoft software.	Trade marks. Copyright.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Vendors located in Germany and Latvia.	Direct sale to customers.	Customers bought copies in good faith, with a presumption that they were authentic.

	Payment methods: the vendors used the payment system made available by third party marketplaces (PayPal). Delivery method: normal shipping. In the court proceedings the claimant presented evidence that the transactions through eBay vendor accounts related to overall activities totalling USD 293 543.	Some customers, after experiencing installation problems, contacted Microsoft for assistance. The vendors provided customers with user manuals. In response to complaints from customers who were dissatisfied with the state of the user manuals, they bought second-hand printed manuals on eBay for the operating system they were selling.
Resilience Against Enforcement Action		
n/a		
Marketing Channels and Internet Traffic Features		
eBay listings.		
Customer Incentives		
Microsoft products were sold at significantly lower prices than the original ones (about three times lower).		

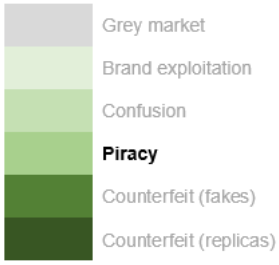
CASE No 12	Vendor Accounts on Third Party Trading Platforms: Sale of subscriptions to major online streaming services

Case study based on an investigation performed by the project team

Date of analysis: 05/03/2021

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



A Greek citizen set up a website selling subscriptions for streaming services. They exploit the fact that a premium version of most of the mentioned services can run on multiple devices. Shared accounts are sold to individuals for a cheap monthly subscription. There are also accounts for VPN services with subscriptions varying from 24 months to 3 years. Affiliate marketing features are also available.

Matrix	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C2	D2	E2	F2
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology

Open internet.

Website controlled by the infringer.

Products and Services

Pirated goods: access accounts to major online streaming services (Netflix, HBO Max, Spotify, Tidal, etc.) and to VPN services (Surfshark, NordVPN, IPVanish VPN premium).

Involved IPR(s)

Copyright and related rights.

Identification of Infringer

Vendor located in Greece.

Revenue Sources

Sale of monthly or yearly subscriptions to customers.

Payment methods: PayPal, credit card.

Instant delivery.

Customer Relations

There is an active server on Discord with many users, increasing day by day. Members communicate daily and report any problems or make requests related to the shared accounts. There are also giveaways to keep members engaged.

Resilience Against Enforcement Action	
n/a	
Marketing Channels and Internet Traffic Features	
Instagram account and Facebook page.	
Customer Incentives	
Cheap streaming services, sense of community with active members and giveaways.	

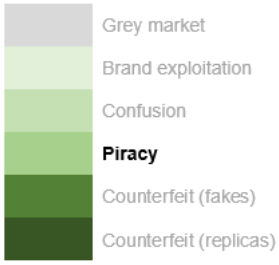
CASE No 13	Vendor Accounts on Third Party Trading Platforms: Vendor of subscriptions to pay-TV and online streaming services

Case study based on an investigation performed by the project team

Date of analysis: 27/02/2021

Based on 'Business Model Canvas' by Strategyzer.com

Business Model Summary



An individual is selling subscriptions to streaming and VPN services through an e-commerce platform. They promote their online shop on public forums. They have been operating for a long time and their strategy is to change the link of their shop to avoid detection. As described in Case No 6, the accounts offered are shared. Resellers are welcome.

Matrix		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C2	D2	E2	F2
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform & Technology	**Products and Services**	**Involved IPR(s)**
Open internet. E-commerce platform.	Pirated goods: access accounts to major online streaming services (Netflix for different countries, such as Denmark, France, Germany, UK, USA; Disney+).	Copyright and related rights.
Identification of Infringer	**Revenue Sources**	**Customer Relations**
Unknown.	Sale of monthly or yearly subscriptions to customers. Payment method: PayPal. Instant delivery.	Contact through email and forums.

Resilience Against Enforcement Action	
n/a	
Marketing Channels and Internet Traffic Features	
Public forums.	
Customer Incentives	
Affordable prices and a 5-month warranty with support.	

EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

VENDOR ACCOUNTS ON THIRD PARTY TRADING PLATFORMS

RESEARCH ON ONLINE BUSINESS MODELS INFRINGING INTELLECTUAL PROPERTY RIGHTS – PHASE 4

Report

ISBN 978-92-9156-298-5 doi:10.2814/279240 TB-09-21-391-EN-N