**Draft categorisation of IP threats - how intermediary services are being misused for IP infringements**

1. **Background and purpose**

The work of the Expert Group on Cooperation with Intermediaries (EG) has led to the publication of several discussion papers identifying trends and challenges in the misuse of different types of intermediary services for IP infringements and setting out good practices to address these misuses.[[1]](#footnote-1) We believe that these papers cover the main intermediary services that are being misused for IP infringing activities and aim to change the approach of this work.

We see a need to move from a sectorial approach to a more horizontal approach through the development of a repository containing all threats/trends and good practices already identified. This will allow interested parties to get a better overview of where overlaps and differences exists. The idea is to update this repository on a regular basis with emerging threats/trends but also with new implemented good practices. The repository will also contain details about relevant legislations where applicable.

In addition, this repository could be used to monitor the evolution of online IP infringement and good practices, as well as share intelligence with IP right holders, law enforcement and judicial authorities, and inform the public on latest online IP threats. This can include support to the Commission in their enforcement activities related to the Digital Service Act and contribute to their Counterfeit and Piracy Watch List.

The purpose of the draft categories outlined in this document is to gather feedback from the EG and IPDW members on the taxonomy that serves as a first basis for the new repository, keeping in mind that threats/trends constantly evolve and that some may change and/or be added in the future.

**Input required:** Stakeholders are invited to comment and make concrete suggestions on the different categories of threats/trends and their definitions, as well as any categories that may be missing. Ideas on ways to ensure the repository will reflect the full range of existing threats/trends, including suggestions on the best way for the Observatory to gather information on existing and emerging/developing threats/trends, are also welcome.

**Next steps:** After this first categorisation, the list of threats/trends already identified as part of the work of the EG will be put into the repository. In addition, we will invite again the EG and members of the broader Observatory network to feed in missing and/or new threats/trends to the repository.

1. **Proposed categorisation**

The proposed categorisation contains concrete lists of examples of identified threats/trends through the work of the EG. This list is non-exhaustive and EG and IPDW members are welcome to add additional examples of threats/trends that may help refine the definition of the categories and subcategories already provided.

IP Threats

[Production and sourcing 4](#_Toc201221215)

[o **Production and acquisition of infringing goods** 4](#_Toc201221216)

[o **IP infringing resource** 4](#_Toc201221217)

[Transportation 4](#_Toc201221218)

[o **Contamination strategy** 4](#_Toc201221219)

[o **Full concealment strategy** 5](#_Toc201221220)

[Storage and Distribution 5](#_Toc201221221)

[o **Storage as an IP infringing action** 5](#_Toc201221222)

[o IP infringement as a service: 5](#_Toc201221223)

[Promotion 6](#_Toc201221224)

[o **Promotion of IP infringing goods and services** 6](#_Toc201221225)

[Monetisation and financing of IP infringing activities 7](#_Toc201221226)

[o **Consumer engagement** 7](#_Toc201221227)

[o **Malicious advertising** 7](#_Toc201221228)

[o **Technical means of payment** 7](#_Toc201221229)

[Evasion techniques 8](#_Toc201221230)

[o **Obfuscation of identity** 8](#_Toc201221231)

[o **Resilience measures** 8](#_Toc201221232)

[Customer relations 9](#_Toc201221233)

[o **Cooperation with other IP infringing persons or organisation** 9](#_Toc201221234)

[o **Cooperation with consumers** 9](#_Toc201221235)

# Production and sourcing

|  |
| --- |
| The misuse of intermediary services by IP infringers to acquire raw materials, including pirated digital content, as a basis for production of IP infringing products or services. This category includes the production of counterfeit products, semi-completed products (e.g. labels) on various scales. |

## **Production and acquisition of infringing goods**

Methods used by IP infringers to produce and or/acquire infringing goods from upstream intermediaries:

**Examples:**

* Internal sourcing of IP infringing materials (acquisition of partial/completed goods, machinery, labelling etc. directly from the manufacturer, aided by past/current employees.)
* Purchasing third party counterfeit/pirated materials (acquisition of infringing audiovisual content, software and or physical goods from third party vendors)
* Assembling/re-packaging/re-labelling after transportation (e.g. transport and logistics)

## **IP infringing resource**

Resources used to produce and/or source infringing goods from upstream intermediaries

**Examples:**

* Human resources (network of individuals involved in producing infringing goods, whether voluntarily or without actual knowledge of the illegal nature of the production)
* Technical resources (all technical measures involved in acquiring infringing content from upstream intermediaries. This includes, but is not limited to, hard drives, cloud hosting services, AI etc.)

# Transportation

|  |
| --- |
| The misuse of transportation and distribution intermediary services to move IP infringing goods (e.g. pharmaceuticals, food, alcohol, clothing) from the production and acquisition stage to its final market. This covers downstream activities involved with transporting goods from production to the final consumer. It includes circumstances where bad actors conceal the infringing nature of the goods being transported through legal means and legitimate businesses. Conversely it refers to the use of wholly illegal means to transport goods via underground supply chains. |

## **Contamination strategy**

The exploitation of legal marketplace distribution channels and free trade zones to transport physical infringing goods.

**Examples:**

* Sending branded logos, labels, tags, packaging and unbranded goods separately to avoid detection (e.g. transport and logistics)
* Undervaluing the goods shipped (e.g. transport and logistics)
* Misclassifying goods shipped (e.g. transport and logistics)
* Exploitation of transhipments

## **Full concealment strategy**

The use of illegal marketplace distribution channels to transport physical infringing goods. Transportation may be aware of the infringing nature of the goods being transported.

Example:

* Direct distribution from infringer to final retailers of IP infringing goods (B2B within the same trade zone/region and/or B2C within the same trade zone/region e.g. transport and logistics)
* Shopping services through apps, where a third party is buying and repackaging infringing goods for their customers

# Storage and Distribution

|  |
| --- |
| The misuse of intermediary services to store, host and distribute IP infringing products both physical and online. Prior to the dissemination of infringing products they are stored in various location, including fulfilment centres operated by e-commerce platform. Storage also encompasses exploiting online intermediaries by uploading IP infringing content to social media platforms, pirating websites and/or email services (this is a non-exhaustive list). |

## **Storage as an IP infringing action**

Storage facilities (physical or electronic structures facilitating the storage of IP infringing goods, services and/or content prior or during the distribution of said goods, e.g. storage of hosting servers)

Examples:

* Internal storage facility owned by the infringer e.g. warehouse
* Makeshift storage facility in infringers homes
* Third party storage facility

## IP infringement as a service:

Online distribution of infringing content from infringers to final user devices by way of hosting, apps and other devices (such as HDMI dongles). This is fulfilled by both upstream hosting of infringing content and downstream hosting of infringing content.

**Examples:**

* Content Management Services (services which provide users with a one-stop-shop streaming sites e.g. domain names)
* App Piracy (services providing live and static infringing content via applications using different deceptive measures to distribute such content e.g. apps and apps stores)
* Apps masquerading under a legitimate trademark
* App cloning, including hiding malicious code from users.
* App squatting
* Fake apps
* Disguised as games
* Geographical activated IP infringing apps
* Hiding App availability
* Cyberlockers (internet hosting site that allows users to upload IP infringing content for storing and/or sharing)
* Unauthorised downloading of videos and content
* IPTV
* Subscription-based - IPTV dashboards
* Open IPTV streams - Open web streams

# Promotion

|  |
| --- |
| The misuse of intermediary services by infringers to raise awareness about their products and services with the intention of attracting new and existing audiences. Infringers may conduct this exercise both online and offline. The former requires the use of posters, brochures, word-of-mouth, fake invoices and bills. The latter may involve the use of third-party marketing, ad placement and paid promotions on social media platforms, piracy websites, digital marketplaces or privately hosted websites. The use of legal means to promote illegal products and services may occur without the knowledge of the external third party providing the resource and infrastructure. |

## **Promotion of IP infringing goods and services**

Advertising and marketing techniques with the goal of directing users towards counterfeit goods, infringing services, and pirated content by using deceptive techniques with the aim of generating revenue from users clicks views and interactions (e.g. apps, ads, search engines) including diverting revenues from genuine IP right holders.

Examples:

* Off-platform advertising (e.g. social media)
* Advertise with unauthorised use of trademarks (e.g. social media, domain names)
* Influencer marketing and affiliate marketing fraud
* Cookie stuffing
* Influencers promoting IP infringing goods. (e.g. social media)
* Display marketing (e.g. social media, domain names, ads)
* Banner ads
* Pop-up ads
* Pop-under ads
* Sticky ads
* Rich media ads
* Embedded ads

# Monetisation and financing of IP infringing activities

|  |
| --- |
| The misuse of intermediary services to extract and collect gains from the distribution and dissemination of IP infringing products, services and/or content and the method by which infringers access and/or move revenue gained by IP infringing activities. Payment can be made directly from final customers to the infringer or between two infringers. Technical means of payment include bank transfer, credit/debit card, cash or other means. |

## **Consumer engagement**

Infringers encouraging consumer interaction to generate revenue from consumers engaging with, content, ads, affiliate links etc. This includes using fraudulent ad and/or impression techniques to generate revenue.

**Examples:**

* Affiliated marketing (commission) from VPN subscription kickback.
* Phishing links

## **Malicious advertising**

Infringer operated platforms and/or sites to which display third party deceptive and/or harmful advertisements. Ads may steal private user information, inject malware into the system or redirect users to phishing sites

**Examples:**

* Ad injection (insertion of unauthorised apps into ads into webpages without the consent or knowledge of the website owner and/or user e.g. domain name, apps and apps store, ads to extract revenue)
* Subscription fraud baiting consumers into registering for a subscription to fake scam streaming and/or downloading services to acquire personal and financial data.
* Click fraud (artificially inflating the number of clicks on an ad, physically or with the use of bots, maximising the amount of payment made per click).
* Impression fraud (artificially inflating the number of times an ad has been shown and/or viewed)
* Ad stacking, layering several ads, but the consumer only sees the top one
* Pixel stuffing, placing an ad in a 1x1 pixel on a webpage, while it is not visible to the naked eye the impression will still counts as being displayed.
* Domain spoofing, deceiving advertisers into believe their ad is being places on a quality website but placing the ad on fraudulent websites.

## **Technical means of payment**

The technical and financial means by which infringers generate, process and move their illegal funds. This includes the exploitation of financial institutions, consumers and third-party users, e.g. banking and non-banking payment transfer.

**Examples:**

* Transaction laundering/ unauthorised aggregation using false invoicing and ad revenue fraud
* Billing fraud
* Subscription based transactions: Customers sending short number with the name of a specific plan to subscribe.
* Donations via digital wallets
* Social credit/non-monetary rewards, including the gamification of piracy (win server space, hardware, notoriety etc.)
* Cash transfer, including the use of cross boarder transportation of cash and virtual currencies

# Evasion techniques

|  |
| --- |
| The use of intermediary services to obfuscate their identity and evade detection by law enforcement, online service providers (OSPs ) and rightsholders. It can also include activities in order to obfuscate identities to manipulate consumers into engaging with specific IP infringing services. Specific activities (including technical activities) are made in order to conclude identity and financial fraud, pre-emptive evasion techniques such as hiding, erasing and distracting from IP infringing content. This also includes the use of unlawful use of payment services to obscure the generation and movement of illegal funds because of IP infringing business practices. |

## **Obfuscation of identity**

Deceptive identification practices to distort a user’s identity to evade detection, ensuring the continuity of IP infringing activities.

**Examples:**

* Domain Privacy services (domain name holder listed as the registrant of record but with alternate, valid contact information e.g. a forwarding address, domain name)
* Use of subdomains to ‘hide’ infringing content
* Use of stolen individual or business details
* Obfuscation of identity using a virtual bank account
* Bullet-proof hosting services (services that do not answer information request or notification about users of their sites)
* TOR and VPN both of which anonymise the identity of the end user.

## **Resilience measures**

Technical measures used by infringers to evade detection from rightsholders and online intermediaries to ensure the continuation of IP-infringing activities (by exploiting key functions of intermediary services)

**Examples:**

* Hosting and/or embedding IP-infringing digital content
* Hidden links
* Linking to IP-infringing content on third-party websites
* Ephemeral content (stories which disappear)
* Mirror sites
* Decentralised IT infrastructures
* Bullet-proof hosting services
* Fallback IT infrastructure
* Informing users on circumvention methods
* Cybersquatting
* Typosquatting
* Infringer as the registrant of a website using a previously popular domain name
* Multiple domain registration for a single site
* Use of the name of an infringing site to register a new domain name with a new ‘operator’

# Customer relations

|  |
| --- |
| The use of intermediary services to facilitate the relationship between infringers and their end customers (deceptive as well as non-deceptive relations). Customer relations also dictate the systems or activities allowing IP infringers to provide information and/or access to tools and knowledge to protect and promote their IP-infringing activities. These activities include the setting up of specific formal and informal networks to support active engagement and exchange of information on IP-infringing tips and tricks. This cooperation ranges from public forum pages to private highly organised groups. |

## **Cooperation with other IP infringing persons or organisation**

Cooperation and collaboration between IP infringers to share knowledge on the infringing business model e.g. private groups where infringers share knowledge on their individual IP infringing operations.

**Examples:**

* Controlled access to closed groups (including private chatrooms or accounts e.g. social media, apps and app stores)
* Support forums for IP-infringing services (public chatrooms, subreddits and other website e.g. social media)

## **Cooperation with consumers**

The relationship management aspect of the of the IP infringing business model which allows infringers to provide a communication channel, offering support and customer service framework.

**Examples:**

* Aftersales customer service (e.g. social media)
* Use of private communication and instant messaging services (e.g. social media, domain name)
* Closed groups pointing to ‘hidden’ counterfeit offers on e-commerce marketplaces (e.g. social media)

1. Expert group discussion papers on [Domain names](https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf) (March 2021); [Social Media](https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Social_Media/2021_Social_Media_Discussion_Paper_FullR_en.pdf) (June 2021); [Payments](https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_payment_discussion_paper/2021_payment_discussion_paper_FullR_en.pdf) (November 2021); [Transport and Logistics](https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Transport&Logistics_Discussion_Paper/2022_Transport&Logistics_Discussion_Paper_FullR_en.pdf) (September 2022); [Live event piracy](https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_Live_Event_Piracy/2023_Live_Event_Piracy_Discussion_Paper_FullR_en.pdf) (March 2023). [Apps & App Stores](https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Apps_and_App_stores/2024_Apps_and_App_stores_FullR_en.pdf) (July 2024); [Search Engines](https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf)  (December 2024). [↑](#footnote-ref-1)