**Categorisation of good practices implemented by providers of intermediary services to address the misuse of their services in the context of IP infringing activities**

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 misuses of different types of intermediary services in the context of IP infringing activities, as well as good practices to address such 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 good practices constantly evolve and that some may change and/or be added in the future. The repository will reflect on their adoption and evolution, as well as on the fact that some good practices may be specific to, or can only be scaled by, certain intermediary services due to the nature and function of their services.

The repository will only list good practices from intermediaries going beyond their strict regulatory obligations, including under the Regulation (EU) 2022/2065 (the Digital Services Act (DSA)). When identified good practice consists of going beyond such strict regulatory obligations, references to such underlying obligations may be added as part of the description of the good practice.

1. **Proposed categorisation**

This categorisation of good practices will serve as a first basis to structure the repository, acknowledging that good practices constantly evolve and that some categories may be added in the future. This list is non-exhaustive and EG and IPDW members are welcome to add additional examples of good practices that may help refine the definition of the categories and subcategories already provided.

**Terms and conditions**

|  |
| --- |
| Provisions applying to the user of the service and establishing the conditions under which they can be used. This includes any contractual conditions that can be imposed by the intermediary on its final users, but also on upstream[[2]](#footnote-2) services through different sources (e.g., Terms and conditions, IP policy, acceptable use policy etc.), as well as conditions prohibiting certain types of content, usages, activities or practices as part of the intermediary service, outside of any contractual relationship. |

* **IP related policy as a condition of use:** Provisions defining acceptable or prohibited uses of the service in relation to IP protection and IP enforcement to inform users and undermine IP infringing activities in general.
* **Policy to respect specific IP rights:** Provisions definingrestrictionsand/or due diligence process to undermine activities infringing specific IP rights or supporting such activities.
* **Policy facilitating IP enforcement:** Provisions defining actions from the providers of intermediary services that they can take against suspicious/alleged or actual IP infringing activities and/or IP infringers.
* **Policy to disincentivize IP infringing activities or compensate affected users.**

Know Your Customers (KYC)

|  |
| --- |
| Verification of the identity and/or identifiers of the user of the intermediary service, including verification of individual or professional users, as well as verification applying to certain business activities, functionalities and/or based on specific use threshold. Verification can be performed by internal or external tools and based on information provided by the users, information held by the providers of intermediary services, as well as external sources of information. This may include practices developed by providers of intermediary services that go beyond the obligation on the traceability of traders under Art. 30 DSA, as well as practices from intermediary services covered by this obligation and that form part of their “best efforts” to assess if the information provided by users is reliable and complete (Art. 30.2 DSA). |

* **Identity and contact detail verification:** Verification of identification information provided by a user throughsingle or multiple identifiers and methods.
* **Identity and contact details verification for businesses:** Verification of legal entity and/or legal representative information provided by the user through single or multiple identifiers and methods.
* **Identity verification for specific activities:** Initial or additionalverification of the information provided by the users in case the service is used for activities that are regulated or present IP-related risks, as well as for the use of specific functionalities oruse over certain thresholds that may present specific IP-related risks.
* **Verification against information other than the one provided by the user:**

Initial or additional verification of the information provided by the user at registration against the intermediary service’s own information, external sources of information, or through specialised verification services.

**Risk assessment systems to detect suspicious activities or users**

|  |
| --- |
| Systems to proactively detect suspicious IP-infringing activities or users, requiring follow up action from the intermediary service to establish the actual IP-infringing nature of the activity or user. This includes risk assessment based on multiple information, including information on user account, activities as well as external source of information (e.g., information from other intermediaries, right holders or open-source intelligence (OSINT) |

* **Risk assessment systems to detect suspicious registration:** Systemsassessing users registered identifiers (e.g., domain or app name, or social media username) to detect registration in the intermediary services that may be indicative of a risk of IP infringing activities.
* **Risk assessment system to detect suspicious activities:**

System assessing users’ activities (e.g., financial transaction, origin and destination of the shipment)to detect patterns in the use of the intermediary service that are indicative of a risk of IP infringing use.

* **Multifactor risk assessments system to detect suspicious users and/or activities:**

Systems assessing information from user registration, activities or sourced externally (e.g., OSINT or information from right holders) to detect patterns in the use of the intermediary service that are indicative of a risk of IP infringing use.

**Monitoring systems to detect IP-infringing activities or users**

|  |
| --- |
| Systems to proactively detect actual IP-infringing activities or users, supporting direct action from the providers of intermediary service against such activities or users. This includes monitoring systems building on the intermediary’s own information, as well as information provided by IP right holders, other intermediaries or other external sources. |

* **Monitoring systems relying exclusively on information provided by right holders to recognize their content**: Systems to detect the availability of IP protected content or products that should not be made available on or through the intermediary service, and that rely exclusively on information provided by right holders.

* **Monitoring systems relying on single or multi-factor detection of IP infringing activities and/or users**: Systems that build on the intermediary services’ experience in handling IP infringing activities and users on its service (incl. through notifications of IP infringement from right holders and other users) to recognize different signals (e.g., keywords, images, logos, IP addresses) or patterns that are indicative of such activities.

**Notification systems**

|  |
| --- |
| Processes and/or systems facilitating the notification of IP-infringing activities or users to the intermediary services, and that are available to different types of stakeholders (incl. but not limited to other users, IP right holders or law enforcement authorities This includes but is not limited to the notice and action mechanisms provided for by the DSA and the CDSM that go beyond strict regulatory requirements (e.g., systems allowing notification in bulk).This does not include IP protection portals or similar systems that require notifiers to register with and sign into a specific system (which are covered in good practices related to cooperation with specific right holders. |

* **Notification systems by intermediaries covered by Art. 16 of the DSA**:Systems that go beyond the strict regulatory obligations to have notice and action mechanisms under Art. 16 DSA, and that aim at streamlining notification of IP infringing activities or users.
* **Notification systems by intermediaries not covered by Art. 16 of the DSA**:

Systems that support notification of IP infringing activities by intermediaries that do not fall within the scope of the DSA but put similar systems in place on a voluntary basis and/or to meet other regulatory requirements (e.g., Anti Money Laundering (AML) obligations).

**Cooperation with specific IP right holders**

|  |
| --- |
| Processes allowing IP right holders to provide information and/or access tools to protect their IP rights on intermediary services. These processes build on active cooperation with clearly identified right holders (or their representatives) and include the setting up of specific right holders’ networks to support active engagement and exchange of information, and/or the development of specific IP protection portals facilitating enforcement and exchange of information (beyond notice and action process covered by Art. 16 DSA). |

* **Selected rights holder networks:** Structured cooperation between an intermediary service andselected right holders to support regular engagement and exchange of information.
* **Systems and/or tools for right holders meeting certain conditions or requirements:** Restrictedaccesssystem for right holders meeting certain requirements and agreeing with terms of use, to gain access to a set of tools to enhance enforcement of their rights, by supporting sharing of information with and/or direct action from an intermediary service.

**Cooperation with public authorities**

|  |
| --- |
| Collaborative efforts from intermediary services to actively engage with public and law enforcement authorities to share or gather information on IP infringing activities and/or infringers, as well as support or initiate specific legal actions against users misusing their services. This includes proactive cooperation in the context of specific operations initiate by law enforcement authorities with the support of right holders, sharing of information as well as use of information made available by authorities. This does not extend to law enforcement portals put in place by some intermediaries to streamline legal requests for information from enforcement authorities to intermediaries. |

* **Participation in specific law enforcement investigations and/or judicial actions:** Intermediariescooperating in law enforcement investigations related to IP infringement.

* **Voluntary collaboration on information sharing:** Collaborations in specific areas focused on information and intelligence sharing with public and/or law enforcement authorities.
* **Voluntary collaboration on information gathering**: Collaboration in specific areas to take into account information provided by public or law enforcement activities.

**Voluntary sectorial or cross-sectorial cooperation agreements**

|  |
| --- |
| Voluntary cooperation agreements between intermediaries from a single or several sectors to support IP enforcement on their services. Such agreements may involve private companies, rights holders, law enforcement authorities, trade associations, as well as national and international public authorities. This includes but is not limited to a Memorandum of understanding or Code of Practice. |

* **Voluntary cooperation agreements between intermediary services.**
* **Voluntary cooperation agreements between intermediary services and right holders.**
* **Voluntary cooperation agreements between intermediary services, right holders and public authorities.**

**IP Awareness campaigns / communication**

|  |
| --- |
| Specific communication and/or campaigns directed at users of intermediary services with the view to actively raise awareness on IP, the risk associated with certain IP infringing activities, and/or the availability of legal services. This includes campaigns or messages developed at the sole initiative of an intermediary service or in cooperation with right holders and/or public authorities. This does not include information resources on IP made available by intermediary services but that are not actively promoted (e.g., IP policy). |

* **IP awareness campaigns / communications from intermediary services**: Campaigns or communication directed to all or specific users of the intermediary services.
* **IP awareness campaigns / communication from intermediary services developed in cooperation with right holders and/or public authorities:**

**Development of judicial and/or administrative borders supporting IP enforcement**

If the rest of the categorisation is exclusively about good practices from intermediaries to address the misuse of their services in the context of IP infringing activities, this part is related to the development of judicial or administrative processes supporting IP enforcement that are directed at intermediary services, and in some instances may require their cooperation to be effective.

**Judicial processes supporting IP enforcement – blocking injunctions**

|  |
| --- |
| Legal mechanisms supporting IP enforcement against various IP infringing activities and/or tactics used by IP infringers to evade enforcement measures, for online piracy, including on live events. Blocking injunctions may require that the blocking occur at domain or IP address levels, and they may be extended by the court in a dynamic manner to cover future locations without the need of requesting a new injunction. |

* **Blocking injunctions**: Requiring online intermediaries to prevent or disable access to IP infringing service or content.
* **Dynamic blocking injunctions**: Requiring online intermediaries to prevent or disable access to IP infringing services or content, and that can be updated to adapt to the measures put in place by IP infringers to defeat blocking.
* **Dynamic injunctions** **used for live events piracy**:Requiring online intermediaries to prevent or disable access to IP infringing services or content for a limited period of time but over an event series (e.g., temporary blocking during all football games of a specific championship). In some instances, live updates also allow for new services to be identified and notified to intermediaries for blocking within a short period of time.

**Judicial order supported by administrative intervention**

|  |
| --- |
| Administrative processes following a judicial order, initiated by rightsholders, supporting effective IP enforcement against different types of IP infringing activities and/or tactics used by IP infringers to evade enforcement measures. This includes injunctions, including dynamic, issued against intermediaries by the judiciary with support from an administrative or regulatory authority. |

* **Administrative process for the enforcement of a judicial order:** Following a blocking injunction by a court, an administrative or regulatory authority acting as a trusted third party is positioned to ensure the effective implementation of the order.

**Administrative orders supporting IP enforcement**

|  |
| --- |
| Administrative processes, initiated by rightsholders, supporting effective IP enforcement against different types of IP infringing activities and/or tactics used by IP infringers to circumvent enforcement measures. This includes administrative authorities with regulatory powers to issue fines, blocking orders and/or injunctions that require ISPs to end IP infringement on their service~~.~~ |

* **Administrative orders:** This includes administrative authorities with regulatory powers to issue fines, blocking orders and/or injunctions that require notably ISPs to end IP infringement on their service.

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)
2. Upstream services may be required to use the intermediary service (e.g., domain name registrar(s) with registry, or acquiring banks with certain payment services) or simply be used by the user (e.g. a privacy or proxy service to register a domain name) [↑](#footnote-ref-2)