Hosting Intermediary Services and Illegal Content Online

An analysis of the scope of article 14 ECD in light of developments in the online service landscape

van Hoboken, J.; Quintais, J.P.; Poort, J.; van Eijk, N.

DOI
10.2759/284542

Publication date
2018

Document Version
Final published version

European Commission

HOSTING INTERMEDIARY SERVICES AND ILLEGAL CONTENT ONLINE

An analysis of the scope of article 14 ECD in light of developments in the online service landscape

Digital Single Market

European Commission

FINAL REPORT

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

Digital Single Market

This study was carried out for the European Commission by

Authors:

Joris van Hoboken (Institute for Information Law (IViR), Faculty of Law, University of Amsterdam; Research Group on Law Science Technology & Society (LSTS), Vrije Universiteit Brussel), João Pedro Quintais, Joost Poort, Nico van Eijk (Institute for Information Law (IViR), Faculty of Law, University of Amsterdam)

Internal identification

Contract number: SMART number 2018/0033

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-79-93002-7

DOI 10.2759/284542

ABSTRACT: This short study looks at the scope of the hosting safe harbour, in view of policies with respect to illegal content online and questions about the scope of Article 14 of the Electronic Commerce Directive (2000/31/EC) from a legal and practical perspective. Specifically, the study addresses the question of what are the kinds of services that could invoke Article 14 ECD and develops an updated typology of hosting intermediaries for policy experts. It outlines the different potential revenue streams of different hosting intermediaries and discusses how these revenue streams may influence the incentives of services to address unlawful or infringing third-party activity. Finally, the study discusses the most important legal issues with respect to the scope of Article 14 ECD, focusing on the case law of the Court of Justice of the EU and other legal developments.

European Commission

HOSTING INTERMEDIARY SERVICES AND ILLEGAL CONTENT ONLINE : An analysis of the scope of article 14 ECD in light of developments in the online service landscape

Luxembourg, Publications Office of the European Union

2018 – 47 pages

EXECUTIVE SUMMARY

The safe harbour framework for internet intermediaries, adopted almost two decades ago at the EU level with the E-Commerce Directive (ECD, 2000/31/EC), has been a core pillar of internet regulation. Harmonized conditional liability exemptions for mere conduit, caching and hosting activities protect information society services from potential strict liability and further the goal of the European single market, provide for legal certainty and strengthen ecommerce, and foster the protection of the rights of internet users, in particular the freedom to receive and impart information and ideas. This short study looks at the scope of the hosting safe harbour, in view of policies with respect to illegal content online and questions about this scope from a legal and practical perspective. After introducing the study in Section 1, Section 2-4 address the following questions:

- What are the kinds of services that could invoke Article 14 ECD and what could an updated typology of hosting intermediaries look like?
- What are the potential revenue streams of different hosting intermediaries and how do these revenue streams influence the incentives of services to address unlawful or infringing third-party activity?
- What are the most important legal issues with respect to Article 14 ECD, in particular with respect to the incentives of hosting intermediaries to address unlawful and infringing activity?

In summary, the landscape of hosting intermediaries has transformed quite significantly since the ECD's adoption. The study presents a typology of hosting intermediaries falling into three broader categories (Category 1: Storage & Distribution; Category 2: Networking, collaborative production and matchmaking; Category 3: Selection, search and referencing).

Article 14 ECD potentially applies to a much larger variety of services than was the case in 2000, with questions remaining about the precise scope and boundary cases. In addition, the economic and societal relevance of the social, cultural, economic, and political processes that are covered have increased significantly. Fundamentally, there is not a single online service or activity that does not involve the activity of one or more hosting providers. This clearly underlines the importance of the ECD's provision and basic EU-level clarifications with respect to their liability. Section 2 concludes with a discussion of activities, other than storage, essential to different hosting intermediaries, to clarify the diversity in the service landscape.

Section 3 discusses the revenue streams, the different illegal content categories and the incentives of hosting intermediaries in this regard. Considering the variety of services covered by the hosting exemption, the differences in size, geographic scope and nature of particular services, the distinctive nature of the illegal content categories and associated policy and socio-legal dynamics, the study concludes that it is hard, perhaps impossible to generalize about the incentives that different services may have with respect to different illegal content categories. The study does provide considerations with respect to the incentives of hosting intermediaries looking at the following topics and perspectives: the severity of risk and harm, the dynamics related to data analytics and platform externalities, the question of innovation and regulatory arbitrage, intermediaries with structural/incidental content issues versus rogue actors, non-profit actors, the size and character of the company offering the services, and finally, the legal framework for hosting intermediaries as it shapes the incentives of relevant services.

Finally, Section 4 discusses the scope of Article 14 ECD from a legal perspective. We signal and discuss some of the most important open questions with respect to the scope of Article 14 ECD, in particular the questions raised by the case law of the CJEU on the required passive or neutral role of hosting intermediaries. We conclude that the terms active and passive/neutral in relation to Article 14 ECD are not to be understood literally or as binary terms but should be understood as legal terms of art that encompass a range of meanings – ascribed by the CJEU (and national courts) – along a potential spectrum of activities performed by intermediaries. Where the intermediary is predominantly passive or neutral, it may benefit from the hosting safe harbour. Where it is active, it will lose that privilege and his role shall be assessed according to national intermediary liability regimes.

The study also concludes that as it stands in the current ECD framework, hosting intermediaries are exposed to a higher risk of liability if they decide to be more active in addressing illegal content in the context of their services, in the absence of what is called a 'Good Samaritan' defence. Overall, we signal a number of legal elements that (will) require (further) legal clarification, including the scope of the definition of information society services in relation to Article 14 ECD, the meaning of active and passive in the case law of the CJEU on Article 14, and the possibility and limitations on duties of care and injunctions, also in view of Article 15 ECD.

1. INTRODUCTION

The safe harbour framework for internet intermediaries, adopted almost two decades ago at the EU level with the E-Commerce Directive (ECD, 2000/31/EC), has been a core pillar of internet regulation. Harmonized conditional liability exemptions for mere conduit, caching and hosting activities protect information society services from potential strict liability and further the goal of the European single market, provide for legal certainty and strengthen ecommerce, and foster the protection of the rights of internet users, in particular the freedom to receive and impart information and ideas.

Article 14 ECD on hosting intermediary activities reads as follows:

> Article 14 Hosting
>
> 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
>
> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
>
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
>
> 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

A number of developments have put pressure on the safe harbour framework, and in particular on the hosting safe harbour (Article 14 ECD). First, the scope of the hosting safe harbour was never as clear as it could have been and over the years the service environment has developed and changed significantly. The social turn (Web 2.0), mobile, cloud computing, the rise of the platform economy, economic consolidation and developments in data analytics have changed the ecosystem and thereby the services that could aim to invoke safe harbours in view of potential liability for third party unlawful or infringing activities.

Second, legal fragmentation in the implementation and interpretation of the safe harbours and developments in related and relevant national and EU level frameworks (e.g. tort law, procedural law, copyright law, criminal law, media law, data protection law) have undercut the goal of legal certainty and the furthering of the EU Digital Single Market. Finally, relevant case law of the CJEU has created certain weaknesses in the safe harbour system. In particular, the safe harbours can be understood to incentivize hosting intermediaries to remain passive in relation to unlawful and/or infringing activities, instead of addressing these issues to the extent technically possible and consistent with service offerings.

This mini-study aims to provide input to address these challenges by answering the following research questions:

1. What are the kinds of services that could invoke Article 14 ECD and what could an updated typology of hosting intermediaries look like?
2. What are the potential revenue streams of different hosting intermediaries and how do these revenue streams influence the incentives of services to address unlawful or infringing third-party activity?
3. What are the most important legal issues with respect to Article 14 ECD, in particular with respect to the incentives of hosting intermediaries to address unlawful and infringing activity?

The overall goal of the study is to provide insights into the question of whether Article 14 ECD is still fit for purpose.

2. A TYPOLOGY OF HOSTING INTERMEDIARIES

2.1 TOWARDS A TYPOLOGY

A typology of hosting intermediaries can provide a starting point for policy discussions about the current legal framework, the issues of tackling illegal and harmful content online as well as the protection of other legal interests, including the protection of the fundamental rights of internet users.[1] More specifically, it can help to clarify the practical scope of Article 14 ECD, which may not be clear to policy makers and legal experts. Until now, the definition of hosting intermediary has not been used in other EU-level laws.[2]

[1] Several larger scale studies on internet intermediaries included such a typology in the resulting reports, but some of the categories are somewhat outdated. See e.g. OECD, *The Role of Intermediaries in Advancing Public Policy Objectives*, 2011; Mackinnon at al., *The Role of Internet Intermediaries*, UNESCO, 2014; EDIMA, Online Intermediaries. Assessing the Economic Impact of the EU's Online Liability Regime, 2012.

[2] The new e-Evidence proposals of the European Commission do contain such a reference. See European Commission, Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. Strasbourg, 17 April 2018, COM(2018) 225 final, available at https://ec.europa.eu/info/sites/info/files/placeholder.pdf (Stating that "The categories of information society services included here are those for which the storage of data is a defining component of the service provided to the user, and refer in particular to social networks to the extent they do not qualify as electronic communications services, online marketplaces facilitating transactions between their users (such as consumers or businesses) and other hosting services, including where the service is provided via cloud computing"). The Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final) also relies on the concept of 'hosting service providers' as delineated by Article 14 ECD.

We will use the following operating definition of hosting intermediary for the purposes of this study:

> *A hosting intermediary is an information society service that consists, amongst potential other activities, of the storage of information provided by a recipient of the service.*

The following criteria were applied in the development of a typology of hosting intermediaries:

- The types of hosting intermediaries need to reflect actual market offerings (accuracy);
- They need to be easily understood by market actors and policy makers (clarity);
- They need to capture the market activities for which the hosting safe harbour could be invoked (adequacy);
- The list of possible hosting intermediary types is meant to provide insight into the landscape of different service types, but should be kept as short as possible (simplification);
- Overlapping categories in the typology cannot be prevented. Some services may fit into two or even three different categories (potential for overlap).

2.2 Developments in the service landscape since the ECD's adoption

Since 2000, when the ECD was adopted, the online service ecosystem has developed significantly. Notable developments include the rise of social media and user-generated content and Web 2.0, the rise of mobile and cloud computing, the increasing economic dominance of the platform model and the collaborative economy. When the ECD was adopted, the landscape of dominant intermediary services looked quite different than today. Most central in the discussion leading to the adoption were the activities of so-called Internet Service Providers (ISPs). These included Internet access providers, which provided access to Internet, and the World Wide Web and Internet hosting providers, which provided the possibility for people and organization to publish a website. The ECD clearly provided for harmonization of the intermediary liability for these services. With respect to Online Service Providers (OSPs), however, intermediary activities were not as clearly addressed by the ECD. Even though a range of OSPs already existed that could invoke the hosting safe harbour (e.g. discussion boards, online marketplaces and classified ads), the ECD remained silent on whether they are included within its scope. Other relevant OSPs that acted as intermediary, e.g. directories and search engines, were left unaddressed, and arguably left out of the ECD's scope.[3]

Whereas ISPs provided the backbone of the Internet service ecosystem in the year 2000, cloud computing does so today. Around 2004, shortly after its adoption of the service-oriented architecture paradigm, Amazon realized that its internal solutions for the production and

[3] See e.g. Van Hoboken, 'Legal Space for Innovative Ordering', International Journal of Communications Law & Policy, No. 13, 2009; See also Van Hoboken, *Search Engine Freedom: On the implications of the right to freedom of expression for the legal governance of Web search engines*, Information Law Series, Vol. 27, Alphen aan den Rijn: Kluwer Law International, 2012.

management of virtual machines could be the basis of an external offering.[4] Amazon's cloud services are leading in the industry. Commercial, consumer-facing Internet-based services are, without much exception, offered over cloud computing infrastructures, which have come to encompass a large variety of different data storage, processing and value-added services to cloud customers.

The rise of social media and user-generated content as a dominant force in the internet ecosystem, happened as a result of a number of factors, including increased access to the internet and the Web for people around the world, the adoption of smartphones with cameras and broadband access and the emergence of new services allowing people to easily connect to friends, family, colleagues and others. The social media and user-generated content services that emerged generally took the open platform approach: they allowed their users to post and share content, bringing them into the scope of hosting intermediaries. More recently, messaging services have come to play an increasingly important role in facilitating group communications in different types of social settings.

Over the last two decades, one can also observe a growing relevance of the platform model in the internet-based services landscape. From search engines to social media, user-generated content platforms and online marketplaces, the so-called multi-sided platform model has become a dominant model for facilitating exchange of value and communications and for generating revenues while doing so.[5] Powerful network effects have turned successful market participants into increasingly dominant players, raising questions of appropriate standards for platform fairness and competition, as well as pluralism and diversity.[6] Finally, what is often called the "collaborative" or "sharing" economy, has brought about a new range of internet-based services that allow people to connect relating to various goods and services, for instance with respect to real estate, mobility, labour, vacation, and money lending or even financing investments. Depending on their particular configuration, some of these services may also be able to invoke the hosting safe harbour for their activities.

In summary, the landscape of hosting intermediaries has transformed quite significantly since the ECD's adoption. Not only does the hosting safe harbour potentially apply to a much larger set of services, the economic and societal relevance of the social, cultural, economic, and political processes that are covered have increased significantly. Fundamentally, there is not a single online service or activity that does not involve the activity of one or more hosting providers. This clearly

[4] See Black, Benjamin. "EC2 Origins". Jan 25, 2009, available at http://blog.b3k.us/2009/01/25/ec2-origins.html.

[5] See e.g. Rochet, Jean-Charles, and Jean Tirole. *Two-sided markets: an overview*. Vol. 258. IDEI working paper, 2004. Rochet, Jean-Charles, and Jean Tirole. "Platform competition in two-sided markets." *Journal of the european economic association* 1.4 (2003): 990-1029. For a non-economic perspective on the phenomenon of platform governance, see Gillespie Gillespie, Tarleton. "The politics of 'platforms'." *New media & society* 12.3 (2010): 347-364.

[6] See for example the report 'Digital platforms: an analytical framework for identifying and evaluating policy options', by Nico van Eijk, Ronan Fahy, Harry van Til, Pieter Nooren, Hans Stokking, Hugo Gelevert, TNO report 2015 R11271, 9 November 2015.

underlines the importance of the ECD's provision and basic EU-level clarifications with respect to their liability.

2.3 Hosting Intermediary Typology

The following typology of hosting intermediaries consists of three broad categories. The first is "online storage and distribution". This is the classic hosting service category: services allowing their users to store content online. Such storage will always involve some degree of (potential) distribution. Once certain information is stored online, it can be retrieved on demand at a later stage. There will be variation in the extent to which the online content is made public and whether the accessibility and retrievability of the online stored content is organized for potential third-parties. Basic file storage solutions will typically at least offer their users a sharing feature. Other services may make the content that is hosted publicly available by default. Some may index it and provide a search interface, thereby facilitating and promoting consumption on the platform itself (thus creating further possibilities for monetization through advertising or other means).

The second general category identified in this study is ''networking, collaborative production and matchmaking'. In this category, the central function of the platform is not (merely) to store content online, even though this always remains a part of the service, but to connect producers and users around more complex sets of networked interactions, such as an online debate and discussions, market transactions or the collaborative production of documents and other media.

The third category of "selection and referencing" services, refers to intermediaries that help provide further value, organization and structure to available offerings online. Review or price-comparison sites help consumers to select service providers and producers of their liking. Search engines, like Google Search or Bing, build an index of information and market offerings elsewhere, helping users to navigate the Web and otherwise publicly accessible information. Directories do the same, with a different technical model, gathering links instead of crawling the Web and creating an index. A complicating factor for these types of intermediaries, from a legal perspective, is that information location tools are not as clearly covered under Article 14 ECD as the other two categories of services. In fact, the ECD seems to not have covered these tools, leaving their legal treatment to the Member States and subsequent evaluations by the European Commission (Article 21 ECD). As noted below in Section 4), the Court of Justice of the European Union (CJEU) has not explicitly excluded search engines from the scope of Article 14 ECD and has concluded that advertising features of a search engine can be covered (Google Search).

Within these broader categories of (1) storage and distribution, (2) networking, collaborative production and matchmaking, and (3) selection, search and referencing, the following types of hosting intermediary services can be distinguished:

Category 1: Storage & Distribution

- **Web hosting:** The classic hosting intermediary: providing the possibility to host a website or other internet-based offering. Customers can publish their website through the services managed by the hosting company. Web hosting can vary in the extent to which it provides pre-installed web hosting and publishing features, such as analytics, programming environments, databases, etc. Examples of providers operating in this market are Leaseweb, WIX.com and Vautron Rechenzentrum AG.
- **Online media sharing platforms:** services, that provide an open platform for online publications as well as the consumption of those publications, including images and video (Youtube, Vimeo, Photobucket), music (SoundCloud, Bandcamp), blogging and journalism (Medium, Wordpress) and other forms of media.
- **File storage and sharing:** Services that offer users the ability to store and share different forms of files online (including video, audio, image, software and text documents). These services range from offering individual file storage solutions, with limited functionality to share, to services that incorporate more social features to facilitate sharing of materials between users and/or with third parties, turning them into online media sharing platforms discussed above. Examples of providers offering file storage and sharing services are Dropbox, box.com and WeTransfer.
- **IaaS/PaaS:** Infrastructure as a Service and Platform as a Service cloud computing services offer a cloud-age version of Web hosting for organizations to run services and applications and making them available to online users. (Notably, these services can themselves act as intermediaries, creating a situation of double hosting.) Examples are AWS (Amazon), Google Cloud, Microsoft Azure, but many smaller and niche players exist in the market.

Category 2: Networking, collaborative production and matchmaking

- **Social networking and discussion forums:** services, like Facebook, LinkedIn and Twitter, that allow people to connect and communicate publicly or semi-publicly.
- **Collaborative production:** services that allow users to collaboratively create documents and other forms of media, and make these available to a broader audience. Wikipedia is an example of this, as well as cloud-based word processing tools, such as Google Docs or Office 365.
- **Online marketplaces:** services, like eBay, Marktplaats, eBid and Craigslist, offering the ability to place advertisements, and sell and buy goods, including second hand goods.
- **Collaborative economy:** services that allow supply and demand relating to various goods and services to connect, for instance with respect to mobility (Lyft, BlaBlaCar), labor (Twizzi), travel/real estate (Airbnb, Homestay), and funding (Kickstarter).
- **Online games:** services offering online multi-user gaming environments (with communication features), such as Xbox Live and World of Warcraft.

Category 3: Selection, search and referencing

- **search tools:** online search services, such as Google Search, Yandex, or Baidu, that provide the possibility to navigate the online environment and search for online accessible information and offerings and directories such as dmoz and startpagina.
- **Ratings and reviews:** online services, like Yelp, that provide the possibility to rate and review third-party offerings of various kinds.

2.4 FURTHER CONSIDERATIONS

As a result of the lack of specificity of the hosting intermediary definition and the wide proliferation of different middleman functions in the online environment, there are many difficult boundary cases. In certain cases, hosting intermediaries may (in addition to their hosting activities) perform activities that do not consist of hosting and the existence of hybrid services may also complicate the analysis. For instance, a Web streaming service may offer the ability of live streaming, which to the extent that it amounts to live streaming, may have to be considered a 'mere conduit' activity.[7] On the other hand, it is possible that with respect to certain parts of the service, a hosting intermediary does not take a passive or neutral role but acts as an actual editor, for instance by reviewing all the material that is posted on the platform. In these cases, the service could not be classified as a hosting intermediary for that particular part of the service, but can remain so for the part of the service in which it doesn't take such an active editorial role.

Another complex boundary case is the example of messaging services. Such services facilitate private communications but are increasingly used for social group communications and play an increasingly important role in online content dissemination. Depending on the service architecture and policies, especially as regards confidentiality, security and content moderation, messaging and chat services may fall into one of the safe harbours of the ECD, mere conduit or hosting specifically. Notably, any policies with respect to unlawful and/or infringing content should take account of the fundamental right safeguards with respect to confidentiality of communications.

In the 1990s, the development of the internet service environment was still in its infancy. What was clear was that traditional value chains in the pre-digital world and the ways in which businesses were structured along these value chains, would not be replicated in the digital realm. The safe harbour framework offered legal certainty on questions related to third-party liability for a whole set of potentially different services, the emergence of which was anticipated but not specifically foreseen at the time. It's important to realize that these categories, in effect, generally fell back on existing legally relevant distinctions in the paper-based era, e.g. the general distinction between carriers,

[7] The referencing to a live stream could be categorized as a hosting activity, if the making available of a link to a live stream is included in the hosting category. Similarly, keeping the live stream available for later viewing could be considered a hosting activity. Additional features in the context of live streaming, such as pausing or fast rewind could further complicate the analysis under Article 12-14 ECD.

distributors (secondary publishers) and editors.[8] As regards question of liability, these tended to fall into different categories under relevant principles of national law.

From all the essential operations on third-party information and communication performed by hosting internet intermediaries, the actual definition of hosting service providers under the ECD only contains the operation of 'storage'. As mentioned above, one may assume that distribution is implied by online storage, but one clearly runs into the limitations of the crude definition of hosting intermediary. To make this point more specifically, it may be worth considering some other essential processes with respect to third party information and communication, that are essential to the various different services in the hosting intermediary typology presented above. As discussed in Section 4 in more detail, currently the law does not provide clarity on the question of how these different activities relate to the question of the scope of Article 14 ECD and different interpretations of the law in this respect remain possible under the Directive and the case law of the CJEU.

- **Storage** (storage of third-party data, of any form or kind): the only activity mentioned explicitly in Article 14 ECD;
- **Distribution** (distribution of third-party data): this activity is implied by the definition of hosting activity. Hosting amounts to holding information in online storage at request, thus making the service provider a source for the information thus held in storage;
- **Processing** (processing of third-party data, of any kind): the definition of hosting remains silent on processing of the stored data. In particular as a result of cloud computing, the activity of processing third party information, communications and applications, has become an important phenomenon.[9] Considering the growing set of advanced services for data analytics processing, processing liability questions will likely play an increasingly important role;
- **Networking** (connecting users): the activity of offering networking can create a social layer to the service and may create economic network effects;
- **Collaboration** (allowing multiple users to access and edit the same "stored" data): collaborative features of hosting intermediaries can change the character of the service, in particular as it is likely that versioning and hierarchies with respect to editing and review will need to be established;
- **Matchmaking** (the linking of supply and demand, broadly understood): this activity creates particular dynamics of supply and demand between different (types of) users of the service;
- **Indexation** (the creation of a searchable index): this activity can integrate the offerings of different users, into one offering;

[8] For an up to date discussion of these categories in defamation law in Common Law countries, see Young, Hilary and Laidlaw, Emily, Internet Intermediary Liability in Defamation: Proposals for Statutory Reform (February 1, 2017). Available at SSRN: https://ssrn.com/abstract=3044772.

[9] The definition of remote computing services in the US law related to lawful access to data by law enforcement agencies includes storage and processing of customer data. See e.g. the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), available at https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

- **Ranking** (the application of ranking mechanisms): this activity can be used to facilitate networking, matchmaking and navigation on the service and create opportunities to (de)prioritize particular offerings.

If one adds the dimension of the different value chains different hosting intermediaries are operating in (media, entertainment, ecommerce, education, politics, cultural production) and the different communication models that different services facilitate (one-to-one, one-to-many, many-to-many), one can see that the hosting intermediary definition stands model for a large variety of different intermediation models, with significant differences in their societal and economic implications. These differences also play out in the particular dynamics of potentially illegal or infringing content or communications, as well as the particular incentives and ability of relevant services to address these dynamics. It seems likely, also in view of the legal developments related to the scope of Article 14 ECD discussed in Section 4 that a more in-depth appreciation of these differences and the nature and character of the different types of services that perform intermediary activities may be necessary to better ground the discussion about the liability and responsibility of hosting intermediaries in view of illegal content online.

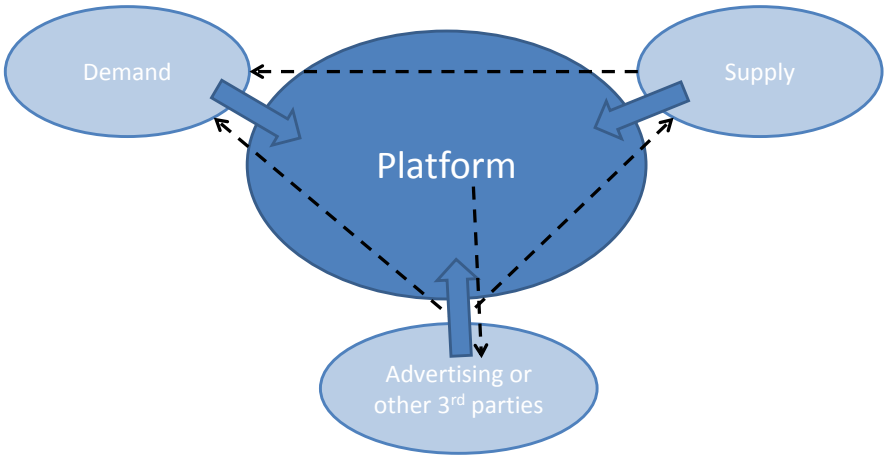
3. BUSINESS MODELS AND INCENTIVES TO ADDRESS UNLAWFUL THIRD-PARTY INFORMATION AND COMMUNICATIONS

3.1 REVENUE STREAMS

To discern the different potential revenue streams of hosting intermediaries, it's valuable to consider hosting intermediaries from the perspective of multi-sided platform markets. Specifically, the model of the 3-sided platform market can capture all the main potential revenue streams, i.e. revenues from the demand and supply side of the platform, plus revenues from potential advertisers and other third parties.[10]

The different forms of revenues are listed and discussed in the text below, the graph below gives a stylized impression of such a three-sided platform, on which supply of and demand for a good or service interact – in case of matchmaking services one party may represent both supply and demand – as well as advertisers or other third parties. Dashed arrows indicate the potential flow of goods, services or information. They all go through the platform, to underscore it is the platform that enables such transactions, if though the transactions themselves may take place elsewhere (e.g. Tinder). Wide arrows indicate potential money flows towards the platform.

[10] In particular areas, there have been some systematic studies of revenue streams. See Incopro, 'The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU', 1 March 2015.



Supply-side revenues:

- **Subscriptions:** It is quite common for online platforms and hosting intermediaries more generally to charge a (tiered) subscription fee to supply-side users of the platform. For instance, a web hosting service, like AWS or Leaseweb, will typically charge a (tiered) monthly fee for hosting a website. Subscription fees are also common for the purchase of additional features, including access to better data (analytics), larger storage capacity, the better targeting of users (Facebook), etc.
- **Transaction fees:** It is common for hosting intermediaries to charge a transaction fee for specific actions taken by the supply-side users of the platform, for instance the creation of an auction on an online marketplace. In the case transactions between supply and demand-side users occur on the platform, it is common that suppliers pay a fee to the platform for facilitating the transaction.
- **Preferential inclusion/placement:** in certain situations, online platforms are in a position to charge preferential treatment to supply-side users. An example is the case of search engines. They can for instance guarantee a certain speed of crawling of new web pages for a fee. The practice of preferential placement (more prominent placement) shifts supply-side users to the category of advertisers, who pay a fee to benefit from the matchmaking function of the platform. Preferential treatment by platforms can create issues from a fair competition perspective.
- **Service fees:** In certain situations, it is possible for online platforms to offer additional services to supply-side users. For instance, the intermediary may have specialized staff to help suppliers optimize their offering on the platform. Depending on their specifics, these services, considering the active involvement of the intermediary with the optimized offerings, may place the intermediary out of the scope of Article 14 ECD.

Demand-side revenues:

- **Subscriptions:** Many online platforms and hosting intermediaries more generally do not charge a subscription fee to demand-side users, at least not for their most basic proposition. Through zero-pricing, the number of users is maximized, thereby optimizing the value of the platforms for

supply-side users and advertisers. Economic theory shows that in many cases (and depending on the supply-side and demand side price elasticities), such zero-pricing strategies lead to maximum overall revenues. There are specific situations in which the end-users are charged a subscription fee, even for passive consumption behaviour. This is the case, for instance, in the area of newsgroups, add-free content services and high-capacity cloud storage.[11]

- **Transaction fees:** When transactions between supply-side users and demand-side users occur on the platform, for instance on Airbnb, payment by demand side users may include a fixed or percentage fee to the platform for facilitating the transaction. When the financial transaction takes place outside the platform, it is more customary that the recipient in the primary transaction (normally the supply-side user) pays such a fee in advance or once the transaction has been completed.

Interaction-related revenues (including advertisers & data brokerage):

- **Advertising (pay-per-click, pay-per-impression, pay-per-transaction):** hosting intermediaries may find themselves in a position to sell privileged access to the users of their service. For instance, online marketplaces can develop sponsored placements. Search engines provide a particularly attractive platform for monetization through advertisement, as the search queries of users can be clear signals of user interests in products or services. Different models for advertisement exist, including pay-per-click (the advertiser pays for each time an ad is clicked by a user), pay-per-impression (payment for each time an ad is shown) or pay-per-transaction (the advertiser pays for when an ad leads to a transaction).
- **Preferential access to data (scraping), including user data:** Some intermediaries may find themselves in a position of having exclusive access to valuable data on users and user interactions, which can be turned into an additional revenue stream.
- **Subscriptions:** whereas advertising and data access revenues may be paid for per transaction, some hosting intermediaries may be able to charge a (tiered) subscription fee to the customers of these services, adding an additional revenue stream.

Revenues, zero-pricing and value creation

A distinction has to be made between actual revenues on the one hand and value creation, more broadly, on the other hand. In the end, revenues – "cash in" - are the basis for any sustainable business model, and thereby fundamental to the incentives structure. Value creation exists when a service creates potential value that can be turned into revenues (or lump-sum buy-out) at a later stage. Value creation, without revenues, or even the perspective of value creation, plays an

[11] For an overview of newsgroup offerings and applicable fees, see e.g. Desire Athow, 'The best Usenet providers of 2018', techradar, 16 May 2018, available at https://www.techradar.com/news/the-best-usenet-providers.

important role in the internet-based service landscape.[12] First, it's very common for online services to first focus on developing a core value proposition and grow the user base, and only later on to start worrying about developing revenues. In many situations, revenue development will only start seriously after an acquisition or when larger investment is needed to keep the service running.

Second, In the context of multi-sided platform markets, value creation on one side of the platform, for instance through an offering to demand-side users with zero-pricing, can be turned into revenues on another side of the platform (supply-side users). This type of value creation is more directly tied to revenues, be it from another side of the platform.

In the absence of actual revenues from end-users, which are a crucial market signal for service providers otherwise, a service provider has an incentive to closely observe the interaction with users and finetune the platform's value proposition towards users in view of optimizing the possibility to monetize on actual user behaviour. In the absence of revenues, one of the concrete ways in which this fine-tuning can take place is on the basis of user data analytics. Different 'types of' users will contribute different value to the platform in terms of revenues and value creation. Some may as well have negative value. A successful platform will want to optimize the value of each user to the total value of the platform and structure their offering to put itself in an optimal position to do so.

So, for instance, a social media user (on a platform that is run on advertisement revenues) that reads other people's posts but doesn't interact herself, will generally contribute less value than a user that posts about life events, invokes interaction with and between others, and creates constructive peer pressure toward users to use the platform to share. A user of an online marketplace that never sends their sold items within a reasonable time period, doesn't take reasonable photographs of the items they sell, thereby creating a suboptimal experience for other users, isn't as valuable as a user that is customer oriented and quick to respond. Users that harass other users, post offensive materials or whose postings constitute safety and security issues may degrade the value of the platform. User data analytics can help the service capture and monitor user behaviour through associated metrics which can also provide the basis for interventions towards users, in the form of general policies and new features.

Additional revenue streams

- **Subsidies:** a variety of hosting intermediaries functions as not-for-profit and receives subsidies (public sector subsidies, private sector, individual donations) to operate. For the purposes of this report, such subsidies can also be treated as a separate revenue stream.
- **Investments (and acquisitions):** some online services may not have any revenues at all, except for the funding they receive from investors. In the area of online service providers, this business model, sometimes denoted with the growth model or acquisition model is widespread.

[12] For a discussion from a competition policy perspective, see e.g. Just, Natascha. "Governing online platforms: Competition policy in times of platformization." *Telecommunications Policy*42.5 (2018): 386-394.

- **Value-added service development:** it is possible that by running the platform, the service ends up being in a position to tap into a related market. For instance, a social network could decide to develop and provide authentication features to other services. A large-scale hosting intermediary could decide to develop and sell access to specialized governance solutions, including illegal/harmful content recognition[13] Cloud computing was first developed by Web native companies to address their own scaling issues and later offered as a new separate service. The large amounts of data and complex governance issues present in internet-scale operating hosting intermediaries, are now leading to the apparent development of artificial intelligence driven tools by some of the largest platforms on the basis of their content moderation strategies, data analytics solutions and related innovations.
- **Commissions:** platforms may also receive a fixed or percentage commission/brokerage fee on transactions that are concluded via the platform, such as a percentage fee on the sale of apps in the IOS App Store or the Chrome Play Store.
- **Reselling of user data and user profiles:** intermediaries can find themselves in a position of having exclusive access to valuable data on users and user interactions, which can be turned into an additional revenue stream in the data brokerage and business intelligence market. Before the actual sale of such data, building a user base and gathering user data can be part of the process of value creation that often precedes actual revenue generation.

3.2 ILLEGAL CONTENT CATEGORIES

- **Copyright and neighbouring rights violations:** copyright (and neighbouring rights) protect creative production by providing the copyright holder a temporary monopoly in the distribution and exploitation of protected works or other subject matter. Liability for copyright protection has been historically among the most important elements of the intermediary liability landscape. A distinction can be made between the unauthorized making available of a copyright protected work on a particular hosting intermediary, and the posting of or availability of links to copyright protected works. A complicating factor in the area of copyright is that there is the possibility that mere hosting intermediary activities could give rise to direct copyright violations.
- **Trademark violations:** trademark protection provides protection against confusing or harmful use of the trademark by third parties. Trademark protection has played an important role in the development of intermediary liability in the area of online marketplaces, social media and search engine advertising.
- **Counterfeiting and parallel distribution:** the phenomenon of counterfeiting consists of the production, distribution and sale of fake products or the unauthorised parallel distribution of real products. Typically, counterfeiting amounts to a number of intellectual property violations (trademark, patents and copyright), in addition to potential non-observance of other applicable regulations.

[13] Additionally, service providers may enter into collaborative efforts with respect to information about (potentially) illegal content, an example of which is the database of hashes hosted by Facebook. See https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/.

- **Trade secrets violations:** trade secret protection consists of the protection of business from unauthorized use of confidential business information. Trade secret violations have not played a significant role in developments related to intermediary liability, but any hosting intermediary facilitating the online storage and distribution of documents could be confronted with a trade secret violation by a user.
- **Consumer protection violations:** consumer protection law consists of a large variety of legal protections for consumers, including sector-specific protections. Consumer protection plays an important role in the area of hosting intermediaries that allow producers to connect to consumers.
- **Privacy, libel and defamation law violations:** privacy, libel and defamation law protect individuals from unlawful intrusions into their privacy (for instance as a result of the publication of private information online), reputation, as well as false, misleading or harmful statements about individuals or business entities. Libel and defamation law traditionally contains special rules on the liability of so-called secondary publishers (libraries, book sellers), which have also been applied to hosting intermediaries.
- **Data protection violations:** data protection law aims to guarantee the fair, lawful and transparent processing of personal data, providing specific restrictions on sensitive data. Data protection law has not played a major role in the development of intermediary (secondary) liability, partly as a result of the fact that hosting intermediaries can still be considered controllers under data protection law, which contains a broad notion of responsibility for the processing of personal data. Search engines, for instance, are considered controllers for the personal data in their search results as a result of people search queries.
- **Hate speech and incitement to violence:** laws on hate speech and the distribution of incitement to violence ('terrorism content'), partially harmonized at the EU level, have gained specific relevance in the area of social media and platforms for user-generated content. Major service providers have signed up to a Hate Speech Code of Conduct and the EU Internet Forum, specifying measures to take down illegal hate speech from their platforms.
- **CSAM and revenge porn:** child sexual abuse material are amongst the most extreme types of illegal content that hosting intermediaries can see themselves confronted with. In the area of CSAM, specific legal and institutional arrangements have been developed, including hotlines and the sharing of hashed CSAM material between law enforcement and service providers. Revenge porn can fall into several other categories of illegal content (privacy, defamation, copyright).

3.3 INCENTIVES WITH RESPECT TO ILLEGAL CONTENT ONLINE

Considering the variety of services covered by the hosting exemption, the differences in size, geographic scope and aims of particular services within each service category, the distinctive nature of the illegal content categories and associated policy and socio-legal dynamics, even within the European Union context, it is hard, perhaps impossible to generalize about the incentives that different services may have with respect to different illegal content categories. Hosting

intermediaries of different kinds can be expected to comply with legal restrictions and duties of care imposed on them with respect to third party illegal content and communications in a way that is in line with optimising expected future revenue streams and/or value creation. Depending on the specific circumstances, this can range from active policing, reactive positioning (shout-if-you-have-a-problem), organizing for plausible deniability with respect to their involvement and knowledge, to going rogue (not making any attempt to be law abiding). Which choice is optimal will depend on the effect of illegitimate activities on the business itself and on related activities (via trust, scaring away supply and demand that does not want to be associated with these activities) and of fear of liability, and other enforcement against the potential damage of that. The following should therefore be understood as an illustration of which perspectives, aspects and factors can be considered relevant when thinking about such incentives from a policy perspective.

Risks and Harms

Clearly, the severity and scale of the potential risk and harm involved in certain forms of content or communications on a platform will have an important impact on the incentives of intermediaries to address and/or prevent it. Not only will enforcement pressure with respect to content or communications that implicates particularly severe risk or harm, be significant and is likely to involve emergency procedures and communication channels, the reputational harm involved in potentially being associated with facilitating access or being the source of such material or activity, will play a role. This is clearly the case of CSAM but severe threats and calls for violence or severe privacy violations can fall in this category, too. Notably, the dynamics associated with potentially severe risk and harm can also create incentives for services to take down content that may be harmful, but not illegal, or incentives not to scrutinize reported content or activity.

Similarly, the risk and harm that the company itself may experience in not addressing certain types of illegal content or activity, will be a primary force in shaping the incentives of intermediaries. This risk and harm can relate to business opportunities in the country or region, including through impacts in business to business relations, the risk of more stringent regulation or litigation, but also the risk to personnel and material assets in a specific jurisdiction.

Data Analytics and Platform Externalities

While generally speaking, every additional user of a platform will contribute to (potential) additional revenues, certain users may actually lower the value of the platform or create risks for the sustainability of the platform in the long run. For instance, users of an online marketplace that defraud other users have a direct negative impact on trust. The online marketplace will have an incentive, in addition to its incentive stemming from the applicability of laws against fraud, to proactively set and enforce policies against fraud. This can be generalized to the situation of illegal or harmful content that creates negative externalities on the platform. The experiences of users of hosting services are not the same, of course. There is a likelihood that the behaviour and experience of the majority of users, or a minority of the most profitable users, end up dictating the choices of a platform.

There are several potential counterweighting incentives at play here, too, pushing back on the incentives of hosting intermediaries to address particular negative externalities. First, to address these issues may involve substantial additional costs for the intermediary. Second, the function of the platform and its position in the value chain may create a strong incentive not to take certain measures. For instance, in the case of search engines, which have a primary role in helping users to find the location of content and offerings elsewhere on the Web, a takedown of a website from the index harms the core function of the platform, i.e. navigation.[14]

Third, the proactive policing measures and enforcement practices may diminish the value proposition towards (certain) users, including through harming their fundamental rights to enjoy freedom of expression, data protection, privacy and due process, and may lead them to switch to other services that act less restrictively. The strength of the network effects and competition with other platforms, finally, can create a strong incentive not to lose any of one's users too easily. It should be noted in this context, that this may create an incentive for hosting intermediaries not to be fully transparent about the restrictive measures they take, highlighting the value of transparency about practices tackling illegal content and content moderation more generally.[15]

It can be the case that the third-party publication and sharing of illegal content or communications creates certain 'positive' externalities on the platform, while harming others and/or societal interests more generally. In the area of copyright infringement, for instance, the users of the platform generally benefit from the availability of content, regardless of whether it was posted there lawfully. For an online marketplace, there may be no inherent strong incentive to tackle the sales of fake items, as long as the sellers and buyers remain happy about their interaction. There may be strong counterweighting incentives to tolerate illegal content dynamics to a certain extent, however. First, the reputational damage of facilitating illegal content online can be considerable and seems to have grown over the years. Second, specific revenue streams, for instance those resulting from deals between platforms and copyright holders, may create an incentive to address copyright violations more actively. Advertising revenues generally create an incentive for intermediaries to address illegal contents, since (most) advertisers will not want to be associated with illegal (or harmful) content.[16]

INNOVATION AND REGULATORY ARBITRAGE

Networked connectivity and socio-technical developments more generally, have created a vibrant ecosystem for innovation, including through the invention of new forms of intermediation. These

[14] The right to be forgotten, as applied by the CJEU in the *Costeja/Google Spain* ruling, is an example, where the service was resisting to take down links to content hosted elsewhere. The application of the right to be forgotten can also create issues for information providers, including newspapers, that see the dissemination of material restricted without a clear process respecting their interests.

[15] See Roberts, Sarah T. "Digital detritus:'Error'and the logic of opacity in social media content moderation." *First Monday* 23.3 (2018).

[16] See e.g. Suzanne Vranica, 'Unilever Threatens to Reduce Ad Spending on Tech Platforms That Don't Combat Divisive Content', *The Wall Street Journal*, 2018.

innovations, like often is the case, can have a significantly disruptive effect on existing value chains. The disruptive potential of innovative intermediary models can involve incentives for new service providers to strategically position themselves more favourably in relation to existing legal and regulatory frameworks than incumbents operating in the market. In certain situations, new service providers may be able to position themselves in such a way that existing laws and regulations in the underlying market do not clearly or effectively apply to them at all. This points to the potential for regulatory arbitrage, including as a result of the safe harbours in the ECD.[17] In situations of regulatory arbitrage, new intermediaries may gain an advantage over regulated entities operating in the same markets. Regulatory arbitrage appears especially widespread in the area of the collaborative economy.[18] The question of where to draw the line between innovation and mere regulatory arbitrage is difficult to answer and will depend on the context and what counts as innovation.

INTERMEDIARIES WITH STRUCTURAL/INCIDENTAL ILLEGAL CONTENT ISSUES VERSUS ROGUE ACTORS

When intermediaries see themselves confronted with usage of their service that is illegal, they may choose to address these issues and limit such usage of their service as much as possible.[19] Typically, this will not result in the full prevention of relevant illegal content or communications, but the issue will be limited to incidents that can be addressed with appropriate policies in place. At the same time, it is clear that certain intermediary actors may deliberately choose not to act at all, but find ways to keep facilitating the unlawful interactions on their platform and turn a blind eye to the extent that it is, or for as long it is, legally feasible. On the one hand, there can be services that do so for principled reasons, arguing that it is not their responsibility to address the respective issues more forcefully. On the other hand, there may also be rogue actors that deliberately optimize their services for a particular type of illegal content or communication. It's important to note that such rogue actors act under a different logic and incentive structure than other market players. They will generally face problems if they wish to enter into relevant business-to-business relations. For instance, they may not find intellectual property owners willing to enter into business relationships with them or will not be able to monetize as effectively through advertising as other services and will,[20] in certain situations, even have to opt for different payment mechanisms, for instance through the use of crypto-currencies if credit card companies refrain from doing business with them.

[17] For a discussion in the area of copyright, see Garcia, Kristelia A., 'Copyright Arbitrage', *California Law Review*, Forthcoming; U of Colorado Law Legal Studies Research Paper No. 18-12. March 28, 2018, available at SSRN: https://ssrn.com/abstract=3151776.

[18] Davidson, Nestor M., and John J. Infranca. "The sharing economy as an urban phenomenon." *Yale L. & Pol'y Rev.* 34 (2015): 215. See also Barry, Jordan M., and Paul L. Caron. "Tax regulation, transportation innovation, and the sharing economy." *U. Chi. L. Rev. Dialogue* 82 (2015): 69.

[19] On the phenomenon of content moderation in online platforms, see e.g. Tarleton Gillespie, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, 2018.

[20] And as a result, may end up serving harmful advertising. See Incopro, The revenue sources for websites making available copyright content without consent in the EU, 2015.

Addressing rogue actors effectively also requires a different enforcement strategy than normal market participants.

NON-PROFIT ACTORS

It is possible that hosting intermediaries act under a non-profit model. In these cases, the revenue streams have a very different character, and the income may consist of donations or the service may be self-funded by the service operators. This creates a different incentive structure than in the for profit situation. It's hard to generalize about the incentives of non-profit actors, in particular if one also includes small niche actors and rogue actors. Notably, non-profit actors are not clearly covered under the EU-level safe harbours.[21]

The for profit nature of an intermediary may create some additional incentives to address illegal content, since the service provider may not want to be seen as making money from illegal activities and also due to the profit making potentially being considered relevant in the determination of the liability of the intermediary service, such as in the case of vicarious liability for copyright infringement.[22] Generally speaking, however, the for-profit nature of a service acting as a hosting intermediary should not be considered a negative factor in the determination of liability. In addition, non-profit entities may have at least as strong incentives stemming from reputational harms, as they will run the risk of losing their financial support in the form of donations or other financial support.

SIZE AND CHARACTER OF THE COMPANY OFFERING THE SERVICES

Clearly, the size of the company and the question of whether it offers a single service or a variety of different services in different markets, will have an impact on the incentives with respect to different illegal content categories. For instance, a hosting service offered by a company that is also offering services in the media industry, for instance a TV channel, is likely to have a different posture towards copyright infringement than a company that only offers a Web search engine online.

The scale and geographic scope at which the service is offered will also have a significant impact on the incentives. It's important to realize that the geographic scope of hosting intermediaries has different components. There is the question of offices and establishments, the question of the physical location of where the service is operated from and the question of the geographic spread of the user base. Some of the services, basic cloud computing services for instance, involve operating physical infrastructure in a particular country. This will create additional links with the jurisdiction(s) in which the service is running, with associated impact on the incentives. For many services acting as hosting intermediaries, this is not the case however, as they can be run on the infrastructure operated by cloud services, creating the situation of double hosting. In such situations, the cloud

[21] See Section 4.2.

[22] For a discussion, see for instance Peguera, Miquel, Secondary Liability for Copyright Infringement in the Web 2.0 Environment: Some Reflections on Viacom v. Youtube (September 10, 2010). *Journal of International Commercial Law and Technology*, Vol. 6, No. 1, 2011. Available at SSRN: https://ssrn.com/abstract=1716773.

service provider's terms of service can be expected to create downstream incentives with respect to the treatment of illegal content online by the respective hosting intermediary.

A hosting intermediary operating at a global scale in terms of its user base will be confronted with a large complex variety of legal pressures relating to the problem of illegal content online. Addressing the relevant issues effectively can involve considerable personnel and other operating costs and some form of competition for these resources will take place, in terms of the source of the legal pressure.

Large scale hosting intermediary services generally tend to attract more legal pressure.[23] Additionally, the larger the business value becomes, the more likely the business would be caught and the more it has to lose in the process. In addition, large scale hosting intermediary activity, also in terms of the scale of reports and notices relating to potentially illegal content or activity, also gives the respective service more data to work with when evaluating and shaping their policies with respect to illegal content online and keeping the service free of illegal content, if the service relies on a reactive model to address concerns. It allows the service to learn from and potentially develop exclusive business intelligence, creating a competitive advantage in the market. This is an aspect that is likely to play an increasingly important role considering automation in content moderation and the management of illegal content online more generally.[24]

THE LEGAL FRAMEWORK FOR HOSTING INTERMEDIARIES

The legal and policy framework for hosting intermediaries and their legal liability and regulatory responsibility to address illegal content plays a crucial role in shaping the incentives.[25] In the next Section, we will discuss some particular developments and aspects relating to Article 14 ECD that should be seen in this light. First, a lack of clarity about the legal framework, such as the question of whether Article 14 ECD can successfully be invoked, can have a significant impact on a service's incentives. Generally speaking, if intermediaries fear being held liable, potentially even under criminal law standards, they can be expected to err on the side of caution and take down allegedly illegal material, without proper review.[26] This points to the need for the careful design of

[23] Although, smaller niche players may more easily get confronted with aggressive legal pressure to run them out of business if they are taking a less cooperative stance.

[24] For a recent technical discussion of content filtering tools, see Evan Engstrom and Nick Feamster, The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools, 2017. See also Natasha Duarte and Emma Llansó and Anna Loup, 'Mixed Messages? The Limits of Automated Social Media Content Analysis', *FAT**, 2018. Waseem, Zeerak, and Dirk Hovy. "Hateful symbols or hateful people? predictive features for hate speech detection on twitter." Proceedings of the NAACL student research workshop. 2016; Farid, Hany. "Reining in Online Abuses." Technology and Innovation 19.3 (2018): 593-599.

[25] For a discussion and examples, see Daphne Keller, 'Internet Platforms. Observations on Speech, Danger and Money. A Hoover Institution Essay, 2018.

[26] See for instance Urban et al, who conclude in the copyright context that "Unbalanced liability standards—fear of suit by copyright holders but not users—creates incentives for OSPs to take down material". Urban et al., Notice and Takedown in Everyday Practice, 2017.

intermediary liability standards and associated policies, including effective safeguards for the fundamental rights of internet users.[27] The notice and takedown model for hosting intermediaries that is implied, but not fully specified, in Article 14 ECD, has been shown to create incentives for intermediary services to sometimes to take down content too easily, without proper scrutiny.

In addition to issues with the current legal standards, there is a tradition of governments and policy makers more generally, using the threat of regulation to push for further self-regulatory measures and co-regulatory agreements. This regulatory strategy, sometimes called regulation by 'raised eyebrows', is common place in the area of intermediary liability.[28] The threat of regulation may be one of the most significant factors in shaping the incentives of hosting intermediaries, as the costs of complying with additional regulations and the heightening of risks to the company in not successfully complying with new regulations can create significant risks and costs.

Over the years, increasing pressure has been put on hosting intermediary services to respect the fundamental rights of their users, the right to freedom of expression in particular. Through the Global Network Initiative (GNI), the launch of which coincided with the threat of regulation through the Global Online Freedom Act (GOFA), leading internet companies adopted a set of human rights principles and a self-regulatory framework for complying with them. Thus, hosting intermediaries clearly have some incentives to respect and promote freedom of expression rights, and this will especially be the case for services with a strong freedom of expression-related missions and value propositions. Overall, however, freedom of expression rights of internet users remain fragile. As noted by Urban et al. in a study on notice and takedown in the copyright domain: "Moreover, further expansion of the notice and takedown model, or changes to it, should take into account the fact that targets' expression rights are fragile in a system with strong removal incentives for complainants and intermediaries, but with such limited countervailing incentives to preserve or reinstate improperly targeted speech".[29]

[27] For a recent proposal to balance fundamental rights in the intermediary liability context, see Angelopoulos and Set, Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary

Liability, 2017. On the fundamental rights implications of privatized enforcements, see Angelopoulos et al, Study of fundamental rights limitations for online enforcement through self-regulation, Institute for Information law, 2015.

[28] Recent policy documents at the EU level, including the European Commission Communication on Tackling Illegal Content Online, 2017, and the European Commission Recommendation on measures to effectively tackle illegal content online refer to the possibility of regulation.

[29] See Urban et al., Notice and Takedown in Everyday Practice, 2017.

4. THE HOSTING SAFE HARBOUR: THE LEGAL STATE OF PLAY

4.1 ARTICLE 14 ECD, THE BASICS

EU law on intermediary liability has a basis in the harmonization in view of the internal market. EU law thus harmonizes intermediary liability standards within the EU legal order, but this harmonization is not complete. As noted, Articles 12 to 14 ECD set forth conditional liability exemptions or "safe harbours" for three types of intermediary service activities: mere conduit, caching, and hosting.[30] Article 15 ECD further provides for a prohibition on the imposition of general monitoring obligations on intermediaries. The horizontal nature of the safe harbours means that they apply to a wide array of content, most notably to the categories of illegal content addressed in this report and specified above at 3.2.

Safe harbours do not prevent that intermediaries are required to take measures against the infringement of third party rights, either through injunctions or duties of care. These possibilities result from different provisions in the ECD and other legal instruments.[31] For instance, injunctions against intermediaries whose services are used by third parties to infringe intellectual property rights (IPRs) are available under the Enforcement and InfoSoc Directives.[32] Importantly, injunction claims are limited by Article 15 ECD and as a result of fundamental rights safeguards in the Charter.[33]

Article 14 ECD contains the safe harbour for hosting service providers, and contains a number of conditions. In the first place, a provider has to qualify as an "intermediary service provider" under the ECD. If that is the case, 14(1) ECD states that such a service provider "is not liable for the information stored at the request of a recipient of the service", subject to two alternative conditions. First, if "the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is

[30] For a recent high-level discussion of the safe harbor framework, Sartor Providers Liability: From the eCommerce Directive to the future, Study prepared for the European Parliament, 2017, available at http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf.

[31] See, e.g. Arts. 12(3), 13(2) and 14(3), Art. 18 (on court actions), and Recitals 45 and 48 ECD. NB that the safe harbour applies also to annex claims to the damages claim. See CJEU, 15 september 2016, case C-484/14 - Tobias Mc Fadden v Sony Music Entertainment Germany GmbH (*McFadden*), par. 75. For an in-depth discussion see Husovec, Martin. *Injunctions Against Intermediaries in the European Union: Accountable But Not Liable?*. Vol. 41. Cambridge University Press, 2017.

[32] See, respectively, Arts. 9 and 11 of the Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Enforcement Directive), and Art. 8(3) of the 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 (InfoSoc Directive)..

[33] CJEU, 24 November 2011, case C-70/10 - Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (*Scarlet Extended*), par. 36 ff; C-484/14 - *McFadden*, par. 87.

apparent". Second, if "the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information".[34]

Before further examining these conditions, we must first clarify what type of liability exemption it provides, an aspect linked to the knowledge standards it sets forth. Article 14(1) ECD contains two distinct knowledge standards, with reference to the illegal activity or information stored, [*potentially referring to two types of wrongdoings*]: (i) "actual knowledge" and (ii) "awareness of facts or circumstances" from which the illegality is "apparent", also referred to as "constructive" or "construed" knowledge.[35] The *travaux préparatoires* of the ECD appear to support this distinction, with the result that criminal liability of hosting platforms would require actual knowledge on the part of the hosting service provider, whereas civil liability regarding claims for damages would require solely constructive knowledge.[36]

When a hosting provider meets the conditions above, it cannot be held criminally or civilly liable (under different knowledge standards) for illegal content uploaded by users using his services. If the conditions are not met, the hosting intermediary cannot benefit from the safe harbour. However, this does not mean the service provider will be automatically held liable for the (allegedly) illegally uploaded content. Rather, its liability as an intermediary will have to be determined under largely non-harmonized national rules or doctrines applicable to persons that "do not themselves violate a right, but whose actions or omissions contribute to such violation", for example resulting from the violation of a duty of care.[37] This means that they will typically be evaluated under doctrines of tort law for "indirect", "secondary", "intermediary", or "accessory" liability.

Article 14 ECD has been subject to interpretation by the CJEU in a number of judgments: *Papasavvas* (C-291/13); *Google France* (C-236/08), *L'Oréal* (C-324/09); *Scarlet Extended* (C-70/10), and *Netlog* (C-360/10). As we shall see, the Court interprets the provision and its conditions in such a way as to add a number of elements to its analysis. The following sections examine such elements and discuss the key issues relating to the scope of the hosting safe harbour, as well as the incentives for providers that can potentially invoke the safe harbour to address illegal content dynamics in the context of their services.

[34] This provision contains two terms defined in Art. 2 ECD: 'information society services' are 'services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC' (Art. 2(a)); and recipient of the service' is 'any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible' (Art. 2(d)).

[35] Angelopoulos. Christina. European Intermediary Liability in Copyright. A Tort-Based Analysis, Information Law Series Volume 39, Kluwer, 2016, p. 113.

[36] Explanatory memorandum COM(1998) 586 final, 18.11.1998. See also Angelopoulos 2016, p. 113.

[37] Koelman, Kamiel. 'Online Intermediary Liability', in: P. B Hugenholtz (ed) *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management*, Kluwer Law International (2000), p.17.

4.2 The Threshold Notion of "Information Society Service"

The ECD safe harbours do not apply to services provided by *all* intermediaries, but only to intermediary service providers that qualify as "information society services".[38] This notion therefore also functions as a threshold that must be cleared to invoke EU-level safe harbours, illustrating the character of the ECD as an incomplete harmonization measure. The definition of "information society service" can be found in Directive 2015/1535 (as introduced first by Directive 98/48/EC): "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"; the directive further contains an Annex of services outside the definition's scope.[39] Recital 18 of the ECD clarifies the scope of the definition for the e-commerce area. Services that do not charge their users can still fall under the definition "in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data."[40]

As noted in Section 2, it is possible to distinguish various types of hosting intermediary service activity. In its case law, the CJEU has applied Article 14 ECD to a search engine's advertising service,[41] an online sales platform[42] and a social networking platform.[43] Article 12 has been applied to an Internet (access) service provider[44] and a provider of an open Wi-Fi network.[45]

With relevance to this discussion, the Court has negatively delimited the concept of information society service, by refusing this qualification to Uber, a company providing a smartphone application that intermediates between a passenger and a non-professional driver in the booking of a transport service. In the view of the Court, "[t]hat intermediation service must thus be regarded as forming an integral part of an overall service whose main component is a transport service", and therefore

[38] See Section 4 ECD ('Liability of intermediary service providers'), Arts. 12 to 15.

[39] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

[40] Recital 18 ECD. See also CJEU, 11 September 2014, case C-291/13 - Sotiris Papasavvas v O Fileleftheros Dimosia Etaireia Ltd and Others (*Papasavvas*). The status of not-for-profit intermediaries is unresolved.

[41] CJEU, 23 March 2010, case C-236/08 - Google France SARL and Google Inc. v Louis Vuitton Malletier SA et al (*Google France*).

[42] CJEU, 12 July 2011, case C-324/09 - L'Oréal SA and Others v eBay International AG and Others (*L'Oréal*).

[43] CJEU, 16 February 2012, case C-360/10 - Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (*Netlog*).

[44] C-70/10 - *Scarlet Extended*.

[45] C‑484/14 - *McFadden*.

"must be regarded as being inherently linked to a transport service". Consequently, Uber does not classify as an "information society service" but rather as a "service in the field of transport".[46]

While it doesn't directly relate to intermediary liability or the scope of Article 14, the *Uber* judgment elucidates an important aspect: the ECD's harmonization regime is incomplete. It only harmonizes safe harbours for services by providers – including hosting – that qualify as "information society services". Where a service falls outside that qualification, for instance because it forms an integral part of or is inherently linked to an overall service that is of a different nature and subject to a specific regulation, it does not benefit from safe harbours in the ECD and the question of liability will have to be settled under relevant national law. This limitation of the ECD's safe harbour regime may be particularly relevant for collaborative economy intermediary activities.[47]

4.3 "Active" vs. "Passive" or "Neutral" Role

The determination of whether an intermediary service provider can benefit from a safe harbour for its activities turns on the qualification of its role as "passive" or "neutral", on the one hand, and "active", on the other. These notions have been developed by the Court in *Google France* and *L'Oréal* on the basis of the ECD's wording.[48] In our view, they are not binary terms to be understood solely with reference to their ordinary meaning. Rather, they should be understood as *terms of art* that encompass a range of meanings – ascribed by the CJEU (and national courts) – along a potential spectrum of activities performed by intermediaries. Where the intermediary is predominantly passive or neutral, it may benefit from the hosting safe harbour. Where it is active, it will lose that privilege and his role shall be assessed according to national intermediary liability regimes.

The conceptual distinction between a passive or neutral service activity and "active" service activity[49] was developed by the CJEU on the basis of Recital 42 ECD, a recital that was actually written in consideration of the mere conduit and caching activities of information society services. This recital states that in order to benefit from the directive's safe harbours, "the activity of the information society service provider" must be:

[46] CJEU, 20 December 2017, case C-434/15 - Asociación Profesional Élite Taxi v Uber Systems Spain SL, par. 33-40; CJEU, 10 April 2018, case C- 320/16 - Uber France SAS v Nabil Bensalem, para. 48.

[47] NB that in contrast to the ECD, both the Enforcement and InfoSoc Directives contain broader notions of intermediary, applying to all "intermediaries whose services are used by a third party to infringe", and none of the latter instruments includes a reference to neutrality, as contained in the ECD (see the subsequent section 4.2). The result is a difference in scope of application. In particular, it is noted that injunction relief under the Enforcement Directive (Article 11) is also available in the case of offline intermediaries, as clarified by the CJEU in C-494/15, Tommy Hilfiger.

[48] See Opinion AG Maduro Case … *Google France*, paras 143-145, and Case… *Google France*, paras 113ff.

[49] The pleonasm is worth making explicit.

- (i) “limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient”,
- (ii) of “a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.”

Condition (i) identifies the types of services the recital aims at. Condition (ii) links the qualification of the *activity* of the service provider of those services to a requirement that it is of a certain *nature*: “mere technical, automatic and passive”. It clarifies that to meet that requirement the provider cannot have “knowledge” or “control” over the information at issue.

The wording of condition (i) clearly indicates that the recital was written with mere conduit and caching providers in mind, not hosting. In fact, Advocate General Jääskinen already convincingly made this same point in his Opinion in *L’Oréal*.[50] Still, in what was arguably a mistaken interpretation, the CJEU has relied on the recital to develop the requirement that the activities of hosting providers under Article 14 be of “a mere technical, automatic and passive nature” – a reference to condition (ii) of the recital. However, also this condition makes more sense for mere conduit and caching activities, especially considering that a hosting intermediary by definition has a basic level of “control” over the information that is stored. Such ability to exercise control may result from ownership of the hosting infrastructure or as a result of their terms of service.

Thus, when the CJEU argues in *Google France* that “in the case where the service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored”, it must clearly mean another level of control than the basic level of control inherent in offering data storage on demand.[51] The notion of “control” in Recital 42 ECD could potentially be related to the notion of control in Article 14(2), which clarifies that the safe harbour “shall not apply when the recipient of the service is acting under the authority or the control of the provider.” One possibility would be to interpret “control” as meaning “editorial control”, thereby mirroring the distinction between primary and secondary publishers in defamation law.[52] Such an interpretation, however, creates exactly the type of uncertainty that the safe harbours were arguably meant to resolve, as it is

[50] Opinion AG JÄÄSKINEN Case C-324/09 - *L’Oréal* paras 138-141, maxime 141: “Even if recital 42 of the directive speaks of ‘exemptions’ in plural, it would seem to refer to the exemptions discussed in the following recital 43. The exemptions mentioned there concern – expressly – ‘mere conduit’ and ‘caching’. When read this way, recital 42 becomes clearer: it speaks of the ‘technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient’ (my emphasis). To my mind, this refers precisely to ‘mere conduit’ and ‘caching’, mentioned in Articles 12 and 13 of Directive 2000/31.”

[51] C-236/08 - Google France, par. 120.

[52] For a discussion of common law standards with respect to hosting intermediaries in the area of defamation, see Laidlaw and Young 2017.

not clear what types of (automated) activities (e.g. the enforcement of content restriction standards automated filtering), should count as "editorial control", and which shouldn't.

In light of the language of Article 15, a more persuasive interpretation of Article 14, is that the control element emphasized by the CJEU in its case law must relate to control over the illegality of the content or communication. Such interpretation would lead back to the knowledge requirement already present in the conditions to the safe harbour, adding clarity to the hosting safe harbour regime by avoiding the reliance on confusing and potentially diverging notions.

The application of Recital 42 has led to increased confusion and complexity with respect to the scope of Article 14 activities, which requires resolution. A part of the solution is in reading the case law carefully and against the background of the underlying goals and service dynamics. First, in reading the Court's case law, it emerges that the concepts of "neutral" or "passive" are not absolute. Rather, they encompass a *spectrum of activities* up to a point where the services of a platform must be deemed "active". Second, the grey area of "suspect" activities for hosting platforms, that pull them out of the scope of Article 14, has only partly been elucidated by the Court's case law, through the qualification of certain activities and factors to assess them.

In *L'Oréal*, for instance, the mere fact that the online sales platform eBay "sets the terms of its service, is remunerated for that service and provides general information to its customers" does *not* mean that it plays an active role.[53] However, if eBay assists users in "optimising the presentation of the offers for sale in question or promoting those offers", it must be considered an active platform.[54] The result is that certain activities provided in the context of a hosting service do not cross the line from passive to active: setting the terms of service, obtaining remuneration for that service, or providing general information regarding the service. On the other hand, activities like *optimising the presentation* of offers for sale or *promoting* said *offers* can contribute to the conclusion that the intermediary activity is of an active nature.

The Court has in addition identified factors to help assess the nature of the host service provider's activities. Thus, in *Google France*, it states that the role played by a platform in the *drafting* of a commercial message that accompanies an advertising link or in the *establishment or selection* of keywords *is relevant* in determining whether a platform is active or passive.[55] It will be up to national courts to assess the relevance of such activities for the qualification of the role played by the platform.

In some cases, the qualification of a platform's activities as active or passive/neutral is straightforward. *Papasavvas* provides a clear example of an active platform, using the concepts of

[53] C-324/09 - *L'Oréal*, par. 115. See also C-236/08 - *Google France*, par. 116.

[54] C-324/09 - *L'Oréal*, par. 116.

[55] C-236/08 - *Google France*, par. 118.

knowledge and control.[56] The case concerned a newspaper company publishing its daily online newspaper. The Court found that the company "has, in principle, knowledge about the information which it posts and exercises control over that information".[57] As a result, it cannot rely on Article 14 ECD. In reaching this conclusion, the Court considered irrelevant whether or not access to the website was free of charge.[58] Conversely, in *Netlog*, the Court simply stated that it was not in dispute that a social networking platform stores on its servers information provided by its users and therefore qualifies as a hosting intermediary service. The passive role of the service at stake was not discussed, and therefore assumed.[59]

In other cases, it is less clear, such as it relates to the curating activities of search engines (as link providers) and to online media sharing platforms. Starting with *link providers*, although some countries inside and outside of Europe contain specific safe-harbours for these activities,[60] the ECD does not. Like with notice-and-takedown (NTD) procedures, the future need to examine "the liability of providers of hyperlinks and location tool services" was foreseen in Article 21(2) ECD. In the absence of such a provision, both the CJEU and national courts have dealt with the activities of search engines mostly in the context of the hosting safe harbour, although some Member States' national laws place them under the "mere conduit" umbrella.[61] In particular, the Court's judgement in *Google France* has applied the safe harbour to a search engine's paid-for advertising links, namely Google's advertising service "Adwords"). However, it remains unclear whether the provision by a search engine's of links outside the context of advertising – in its role of providing what are called organic search results – is covered by Article 14 ECD.[62]

[56] C-291/13 - *Papasavvas*.

[57] *Ibid*., par. 45.

[58] *Ibid*.

[59] C-360/10 - *Netlog*, par. 27.

[60] In Spain, see Ley 34/2002, de 11 de julio, *sobre servicios de la sociedad de la información y comercio electrónico* (LSSICE). In the US, see on 'information location tools' sec. 512(d) of the Digital Millennium Copyright Act (17 U.S.C., adopted 28 October 1998); In Canada, the *Copyright Act* shelters most internet intermediaries (as ISPs, hosting services, and search engines), from civil liability for copyright infringement by their users, See Canadian Copyright Act, Secs. 2.4(1)(b), 31.1(1)-(2),(4), and 41.27(1) specifically on information location tools.

[61] See Van Hoboken 2012, for an in-depth discussion of national implementation of the ECD and the qualification of search engine providers in this context.

[62] J. Nordemann, Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?, Study prepared for the European Parliament, 2018. Available at http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA%282017%29614207, pp. 15-16.

The issue is particularly pressing in the context of copyright. In this field, the Court's case law has evolved to encompass the posting of hyperlinks within the scope of the exclusive right of communication to the public (Article 3 InfoSoc Directive), in some cases subject to a knowledge test,.[63] The key case here is *GS Media*. In it, the Court states that where a link provides access to a work published online without the consent of the copyright holder and the person "knew or ought to have known" about that lack of consent, then the hyperlink itself infringes the right of communication to the public.[64] With this move, the Court "introduced a subjective knowledge test in the infringement analysis" of the exclusive right, making its application in some scenarios dependent upon a requirement of intent or negligence.[65] For links pointing to unauthorized content, where actual knowledge is not established, the Court devised a rebuttable (*juris tantum*) legal presumption, which presumption depends on whether the posting of hyperlinks is carried out for profit. According to this, "if the posting of hyperlinks is carried out for profit, it can be expected that the person who posted such a link carries out the necessary checks to ensure that the work concerned is not illegally published on the website to which those hyperlinks lead, so that it must be presumed that that posting has occurred with the full knowledge of the protected nature of that work and the possible lack of consent to publication on the internet by the copyright holder". Failure to rebut the presumption leads to the qualification of the link at issue as a communication to the public under Article 3 InfoSoc Directive.[66]

One consequence of this interpretation with relevance here is the potential application of the exclusive right to to link aggregators, like search engines. While this is an on-going debate, it is worth noting a recent decision by the German Federal Court on a case concerning links in the context of search engines, more specifically thumbnails of pictures available on the Internet without the consent of the copyright holder. The Court ruled that the defendant did not infringe copyright, noting that in case of search engines there is no presumption that the user has knowledge whether the respective content has been published with the consent of the copyright holder or not.[67]

[63] The case law at issue includes judgements on the application of the exclusive right to different scenarions involving hyperlinking to authorized and unauthorized content (*Svensson*, *BestWater, GS Media*), to the sale of kodi boxes *(Filmspeler*), and the provision of an online peer-to-peer file sharing platform (*Ziggo*). For an in depth analysis of this case law and its implications, see J.P. Quintais, 'Untangling the Hyperlinking Web: In Search of the Online Right of Communication to the Public', *The Journal of World Intellectual Property* (forthcoming 2018).

[64] *GS Media*, 49

[65] Senftleben, Martin, Copyright Reform, GS Media and Innovation Climate in the EU – Euphonious Chord or Dissonant Cacophony? (November 6, 2016). Tijdschrift voor auteurs-, media- en informatierecht 2016, pp. 130-133. Available at SSRN: https://ssrn.com/abstract=2865258, p. 132

[66] *GS Media* 51; see also *Filmspeler*, 49

[67] German Federal Court: BGH, Urt. V. 21.9.2018 – I ZR 11/16.

Whereas some commentators welcome this "flexible approach establishing adequate duties of care for linking providers",[68] others rightly note that the Court is using primary liability to indirectly harmonize secondary liability in the field of copyright.[69] This is because current law remains unclear as to whether the activities of certain link providers/aggregators and online media sharing platforms are better qualified as those of copyright *users* or *intermediaries*. As users, they would be primarily liable for acts of making available works under Article 3 InfoSoc Directive. After *GS Media* and *Ziggo*, the scope of direct liability arguably extended to some of these service providers through the application of the knowledge test, the underlying connected presumption and its for-profit condition). If knowledge is established, the service provider cannot benefit from the hosting safe harbour. Only where knowledge is not established, can such providers qualify as mere intermediaries and potentially benefit from the hosting safe harbour, as long as they comply with eventual national duties of care.

Another (related and) debated case is that of large-scale online media sharing platforms, like YouTube or Vimeo.[70] These have for years been qualified by national courts as benefiting from the hosting safe harbour, testing the borders of the passive/neutral spectrum.[71] Importantly, this qualification is sometimes tied to the platform's compliance with duties of care in national law, as well as with the assessment of its knowledge or awareness vis-à-vis the illegal nature of the content hosted.

However, even with such caveats, the qualification of online media sharing platforms as passive is contested on the grounds that the services or activities provided cannot be considered as such, as these platforms have sufficient knowledge or control over the information they store to assess its legal status. In this line, it is possible to find national case law ascribing an active role to online media sharing platforms, thus denying them the protection of the hosting safe harbour. An example is a decision of the Hamburg Court of Appeal on YouTube, considering the platform to be playing an active role when "providing extensive user friendly functions for the use of music provided on YouTube such as search, categories with genres, filtering, marking, playlists, playing functions,

[68] Nordemann 2018, p. 16.

[69] Angelopoulos 2016. See also 'CJEU Decision on Ziggo: The Pirate Bay Communicates Works to the Public'. *Kluwer Copyright Blog*. Available at: http://copyrightblog.kluweriplaw.com/2017/06/30/cjeu-decision-ziggo-pirate-bay-communicates-works-public/.

[70] This issue is at the heart of the current legislative proposal and debate in the context of Article 13 of Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, Brussels 14 September 2016, COM(2016) 593 final. This topic is outside the scope of the present study.

[71] France: TF1 et autres c. YouTube, Tribunal de grande instance de Paris, 29 May 2012; Germany: OLG Hamburg, 1 July 2015, 5 U 87/12. For another case on YouTube as a *Störer* see: OLG München, 17 November 2011, 29 U 3496/11. Spain: Sent. JM n.7 Madrid, 20 Sept.2010; partially confirmed by AP Madrid (sec.28) January 14, 2014 [*Telecinco v. Youtube]* Westlaw.ES JUR\2014\36900.

recommendations to third parties, etc."[72] This case will be decided by the German Federal Court of Justice (BGH) still this year.[73]

To sum up, it can be stated that the notions of "neutral" and "passive" role in CJEU case law are not absolute, allowing the platform to carry out a number of activities in relation to the content they host. The result is that a number of service providers and activities have benefited from such qualification: an internet service provider,[74] a provider of an open Wi-Fi network,[75] a search engine's advertising service, [76] an online sales platform[77] and a social networking platform.[78] National courts have so far mostly endorsed this predominantly neutral or non-active approach.[79] However, there is an undeniable contested area in what concerns the activities link providers and especially online media sharing platforms, which qualification as neutral or active may (and in many cases will) depend on the assessment of their knowledge/awareness and control over the hosted information, as well as their compliance with duties of care under national law.

4.4. KNOWLEDGE AND AWARENESS

As noted above (Section 4.1), Article 14(1) ECD ties the liability of hosting providers to two knowledge standards, the condition of "actual knowledge" or, as regards claims for damages, "awareness' of circumstances regarding the illegal status of the hosted content (a standard commonly referred to as "constructive" knowledge). Hence, the type of knowledge relevant relates to the illegal status of the content. (Knowledge, as noted above, is also a key consideration in determining the active or passive role of a platform.) Upon obtaining actual knowledge or awareness,

[72] Nordemann 2018, p. 10. For additional examples in UK, France, and Germany, see Angelopoulos, On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market, Study for MEP Julia Reda, January 2017, pp.23-30.

[73] See Press Release, BGH, *Verkündungstermin am 13. September 2018, 9.00 Uhr (Verhandlungstermin 22.2.2018) in Sachen I ZR 140/15 (Haftung von YouTube für Urheberrechtsverletzungen)*, http://www.bundesgerichtshof.de/SharedDocs/Termine/DE/Termine/IZR140.html

[74] C-70/10 - *Scarlet Extended*.

[75] C‑484/14 - *McFadden*.

[76] C-236/08 - *Google France*. For a discussion with reference to case law on the legal status of the editorial linking activities of search engines, see Nordemann 2018, pp. 15-16.

[77] C-324/09 - *L'Oréal*.

[78] C-360/10 - *Netlog*. Notably, the CJEU did not consider the question of whether the activities of the service were sufficiently passive and neutral to be able to invoke Article 14 and 15 ECD.

[79] See, for example, OLG Hamburg, 1 July 2015, 5 U 87/12 (in which the German court held that video sharing platform YouTube is a passive provider) and CA Paris, 2 December 2014, *TF1 et autres c. Dailymotion* (where a French court considered video sharing platform Dailymotion passive as well).

a platform has to act 'expeditiously' to take the illegal content down in order to benefit from the safe harbour. The point is reiterated in Recital 46 ECD, which adds that 'the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level'. This recital, furthermore, appears to assume a 'good faith behaviour' model for hosting providers benefiting from the safe harbour.[80]

THE MEANING OF ACTUAL KNOWLEDGE AND AWARENESS

The Court's case law is yet to define "actual knowledge". Natural, the notion excludes "constructive" knowledge, knowledge presumptions or fictions. However, it is less clear if the provision refers to "general" or "specific" knowledge of the illegal activity or information stored at the request of a recipient of the service. In this context, "general" would refer to knowledge about the use of the service to host illegal content, whereas "specific" would relate to knowledge of the illegality of particular items of hosted content. Many platforms will have general knowledge that their service is used for the communication of illegal content, but lack the specific knowledge of concrete infringements, unless notified to that effect.

Historically, European courts have interpreted "actual" knowledge as meaning "specific" knowledge. An illustration of this approach is found in *L'Oréal*, where the CJEU indicated that a notification of illegal content hosted must be sufficiently precise and adequately substantiated for it to yield actual knowledge of the infringement for the host provider.[81] Despite this, some authors have noted a shift towards a more "general" knowledge-based approach.[82] For example, it can be argued that an intermediary does not have to know the identity of the infringer or the infringed copyright-protected work in order to take down the content: more "general" knowledge of the infringement would suffice in this case.[83]

Differently from knowledge, the CJEU had provided some guidance in *L'Oréal* on what constitutes "awareness" within the meaning of Article 14.[84] A platform has awareness "if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised" that the content was unlawful and did not act expeditiously to take it down.[85] For some authors, the awareness standard should be interpreted in light of the model of good faith hosting provider endorsed in Recital 46 ECD, thus allowing courts, on the merits of each case, to refuse safe harbour

[80] Nordemann 2018, p. 11, arguing for the exclusion of 'non-sufficiently collaborative hosting providers' from the safe harbour.

[81] C-324/09 - *L'Oréal*, par. 122.

[82] Angelopoulos 2016, p. 274. See also Nordemann 2018, pp. 11-12.

[83] Angelopoulos 2016, p. 277.

[84] C-324/09 - *L'Oréal*, par. 106.

[85] *Ibid.*, par. 124.

protection to "bad faith" or "non-sufficiently collaborative" hosting providers, i.e. those intermediaries whose business model relies on fostering infringement by their users.[86]

OBTAINING KNOWLEDGE OR AWARENESS

There are two methods to obtain knowledge and awareness. The first is *proactive*, as a result of "investigations undertaken on the intermediary's own initiative".[87] The second is *reactive*, as a result of "information supplied by an injured party or otherwise".[88]

In theory, at least from a purely legal perspective on intermediary liability, there are fewer incentives for intermediaries to engage in proactive efforts to obtain knowledge of the infringement. On the one hand, some types of proactive approaches may lead the intermediary to steer away from passive and neutral model preferred by the ECD and into a qualification as an active host, with the risk of losing safe harbour protection. This is the so-called "Good Samaritan" paradox, further discussed below. On the other hand, certain measures for proactively seeking knowledge of infringements taking place in the platform may contravene the prohibition on imposing general monitoring obligations in Article 15 ECD, and therefore cannot be imposed by Member States on platforms.

Partly for these reasons, it appears that knowledge or awareness will result most commonly from *reactive* methods, such as notices by third parties. From this standpoint, the legal framework incentivizes the adoption of NTD procedures, according to which hosting providers are obliged to remove infringing content they host if notified or lose the benefit of the safe harbour. Although this is far from a detailed procedure, as exists in some countries inside and outside of Europe[89], Article 21(2) ECD foresees the need for *inter alia* more detailed harmonized rules on NTD procedures.

Importantly, not every notification of illegal content received by the platform automatically leads to a loss of safe harbour protection if not accompanied by removal of the content at issue; in other words, the action by the hosting provider following a notice does not necessarily have to be a takedown of the content. In this regard, *L'Oréal* states that a notification "may turn out to be insufficiently precise or inadequately substantiated" to lead to actual knowledge or awareness on the side of the platform, and that it is for national courts to decide whether or not a platform can still rely on Article 14.[90] In this line, national legislators and courts, as well as stakeholders through Codes of

[86] Nordemann 2018, pp. 12-13, mentioning sharehosters as an example of such 'dangerous business models'.

[87] C-324/09 - *L'Oréal*, par. 122.

[88] C-236/08 - *Google France*, par. 109.

[89] In Europe, see e.g.: in Hungary Art. 13 Act CVIII of 2001 on certain aspects of electronic commerce services and of services related to the information society; in Finland, Arts. 20-25 Act 458/2002 on Information Society Services and Electronic Commerce. In the US, see secs 512(c)(1)(C) and 512(c)(3) of the Digital Millennium Copyright Act (17 U.S.C., adopted 28 October 1998)).

[90] C-324/09 - *L'Oréal*, par. 122.

Conduct, have on occasion established minimum requirements for notifications to lead to actual knowledge by the platform.

EXPEDITIOUS ACTION

Finally, it remains unclear what is the precise meaning of "expeditious" action to remove or to disable access to the illegal information. Beyond the ordinary meaning of an action carried out with "speed and efficiency", expeditious may vary along different dimensions relating to the person providing the notice, the content at issue, and the obviousness of the infringement. These dimensions can be illustrated by different examples.

In its Communication on *Tackling Illegal Content Online*, the European Commission does not propose specific timeframes for expeditious action, but states that, in general, notices by "trusted flaggers" should be addressed more quickly than others.[91] Furthermore, in cases where serious harm is at stake, such as content that incites to terrorism, removal can be made subject to specific time frames.[92] In the ensuing Recommendation this point was further specified, with the Commission stating that notices of terrorist content should as a rule be acted upon within an hour.[93]

In national law, one notable example is the German Network Enforcement Act provides for rules according to which an action must be taken within 24 hours after having been notified for content that is manifestly illegal (Art. 3), and within 7 days for illegal content that is less apparent.[94]

Finally, some guidance on the meaning of "expeditious action" can also be derived from Codes of Conduct. For instance, the EU Code of Conduct on Countering Illegal Hate Speech Online requires action by the platform in in less than 24 hours after being notified, whereas the Dutch Notice-and-Take Down Code of Conduct mentions the need for such an action within 5 working days following notification, provided the content is not manifestly unlawful or punishable.[95]

4.5 THE "GOOD SAMARITAN" PARADOX

[91] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms, Brussels, 28 September 2017, COM(2017) 555 final, under 4.1. A trusted flagger is 'an individual or entity which is considered by a hosting service provider to have particular expertise and responsibilities for the purposes of tackling illegal content online'. Cf. Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online, Brussels, 1 March 2018, COM(2018) 1177 final (Recommendation 2018), Art. 4(g).

[92] *Ibid*.

[93] Recommendation 2018, Recital 35.

[94] See, regarding the first, Art. 3, and the second, Art.1, Section 3(3) German Network Enforcement Act.

[95] See EU Code of Conduct on Countering Illegal Hate Speech Online; Dutch NTD Code (explanatory note to Art. 3.a).

The "Good Samaritan" paradox, already briefly described above, relates to the lack of incentive for hosting providers to take proactive measures against infringements on their platform for fear of assuming too "active" a role and, as a result, losing safe harbour protection.[96] Relatedly, Article 15 ECD allows both for the possibility of "specific" monitoring obligations and the adoption of voluntary measures for monitoring and filtering unlawful content.

Scholars are divided on whether the legislative framework should be amended to afford protection to Good Samaritan providers.[97] The Commission, for its part, endorses these measures. The Communication on *tackling illegal content online* states that taking voluntary proactive measures to detect and remove illegal content online does not automatically lead to the online platform losing the benefit of the safe harbour under Article 14 ECD. The point is reiterated in the subsequent Recommendation.[98] The main argument in support of this position is that even if such measures result in obtaining knowledge or awareness of illegality, the hosting platform retains "the possibility to act expeditiously to remove or to disable access to the information in question upon obtaining such knowledge or awareness".[99] Provided it does so, it will not lose the benefit of the safe harbour.

Some case law supports this stance. In Germany, for example, the use by YouTube of its Content-ID software – a paradigmatic "Good Samaritan" "filtering system" – has not led to the qualification of the platform as playing an active role.[100] Similarly, in a Spanish case, the national court concluded that the editorial activities or tasks of YouTube did not mean it had active knowledge of the unauthorised status of the files uploaded by its users, or proactive control over the same.[101]

It is also possible to find examples of Good Samaritan provisions in Codes of Conduct. In the UK, the IPO Code of Practice on Search and Copyright states that "[n]o action undertaken in furtherance of these practices shall impute knowledge, create or impose liability, rights, obligations or waiver of any rights or obligations for any parties."[102] In France, the Charter for the Fight against the Sale of Counterfeit Goods on the Internet provides for monitoring obligations on its parties while stating that the signing of the Charter and implementation of measures therein "shall not prejudice the legal

[96] See, e.g. Nordemann 2018, p. 10; Angelopoulos 2017 [11 ff].

[97] For: Angelopoulos 2017, pp. 43-44. Against: Nordemann 2018, pp. 10-11.

[98] Recommendation 2018, Recitals 25-26.

[99] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms, Brussels, 28 September 2017, COM(2017) 555 final.

[100] Nordemann 2018, p. 10-11, citing OLG Hamburg, 1 July 2015, 5 U 87/12, par. 198.

[101] AP Madrid (sec.28) January 14, 2014 [*Telecinco v. Youtube]* Westlaw.ES JUR\2014\36900.

[102] IPO Code of of Practice on Search and Copyright (UK): Art. 22.

status of the signatories nor their current or future liability regime… [*and*] ...have no consequences on current or future legal proceedings".[103]

There are however some issues with the Commission's proposed interpretation. One is the notion that a proactive approach is less burdensome than the reactive model. This does not appear to be the case. The conditional nature of the safe harbour means that platforms choosing to adopt proactive voluntary measures will have to act upon every instance of illegality they find, as well as to sufficiently justified and adequate notices by third parties. Platforms that adopt a reactive model will only have to take action in the latter case and on those fewer cases where they are (accidentally) aware of illegal content.

The proactive approach leads to an additional problem. The more a platform monitors for illegal content, the more likely it is to find it. In turn, it becomes more probable that the platform fails to identify or adequately take action in relation to some of the illegal content it hosts. For such content, the platform's now "active" role means that it will lose safe harbour protection. Thus, a proactive stance increases the probability that the hosting provider acquires knowledge of the illegal status of the content it hosts and, by extension, its exposure to liability.[104]

The Commission's approach is therefore problematic for hosts, in particular because it does not provide them with a true "good Samaritan" protection. Such a protection is for instance found in Section 230(c)(2) of the US Communications Decency Act,[105] which insulates platforms that monitor for offensive speech from liability when they make their best efforts to moderate content, even if they fail to identify illegal content and thus take any action in relation to it.[106] As it stands in the current ECD framework, platforms are exposed to a high risk of liability in the latter case.

4.6 Injunctions and Duties of Care

As noted, the ECD safe harbours apply to damages and allow for the imposition of injunctions and duties of care. Both injunctions and duties of care are limited in their application by the operation of fundamental rights and the ban on general monitoring obligations.

[103] French Charter for the Fight against the Sale of Counterfeit Goods on the Internet, Par. 6 Preamble and Art. 3.

[104] Aleksandra Kuczerawy, *The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?*, CITIP Blog, KU Leuven, 24 April 2018, available at https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5/.

[105] Communications Decency Act, 47 U.S.C. §230(c)(2).

[106] See Kuczerawy 2018, calling this a 'Good Samaritan 0.5' approach.

INJUNCTIONS

In respect of injunctive relief against intermediaries, EU secondary law on IPRs appears to be the most developed.[107] In the field of IPRs, EU law allows for competent judicial authorities to issue injunctions against intermediaries whose services are being used by a third party to infringe these rights. The general regime for these injunctions concerning IPR infringement is found in the Enforcement Directive, whereas the InfoSoc Directive contains specific rules for copyright infringement.[108] In particular, Article 8(3) of the InfoSoc Directive obligates Member States to ensure that rights holders can apply for injunctions against intermediaries whose services are used by a third party to infringe copyright, even if the intermediary is not itself directly liable for infringement.[109]

The latter provision has played a significant role in the development of the liability of intermediaries, in articulation with the safe harbours in the ECD. In particular, although it is up to national law to determine the scope and procedures to seek injunctions, the same is limited inter alia by the operation of fundamental rights recognized in the EU Charter. This implies that an injunction must strike a fair balance between conflicting fundamental rights: to copyright as property, on the one hand (Article 17(2) EU Charter); and to the protection of personal data and privacy of Internet users, their freedom to impart and receive information, and intermediaries' freedom to conduct a business (Articles 7, 8, 11 and 16 EU Charter).[110]

DUTIES OF CARE

Recital 48 mentions the possibility that Member States impose duties of care on hosting providers. These duties must be (i) reasonable, (ii) specified by national law, and (iii) limited to detection and prevention of certain types of illegal activities.

What exactly constitutes a duty of care may vary according to national law and legal tradition.[111] Among scholars, there has been discussion on the precise meaning of such duties in relation to the

[107] In this respect, we are not qualifying as 'injunctive relief' the measures available in respect of certain particular types of illegal content, such as child pornography (under Directive 2011/93/EU), and in respect of terrorist offences (under Directive (EU) 2017/541), as mentioned in Recital 10 of the Recommendation on Tackling Illegal Content Online.

[108] Art. 11 and recital 23 Enforcement Directive; Art 8(3) InfoSoc Directive.

[109] And, thus, for damages under the first two paragraphs of the provision. See recitals 59 InfoSoc Directive. [CJEU, LSG]. NB that Art. 8(3) InfoSoc Directive remains applicable despite the existence of provisions on injunctions in the Enforcement Directive. Cf. Recital 23, Art. 9(1)(a) in fine and 11, *in fine* Enforcement Directive.

[110] CJEU case law relevant in this respect includes *Scarlet Extended, Netlog*, *UPC Telekabel*, and *Bonnier Audio*.

[111] As Koelman noted already in 2000, a duty of care "may constitute an unlawful act or a tort in itself, or may play a role in the requirement of fault and therefore result in liability". See Koelman 2000, p.11

hosting safe harbour. Edwards, for example, notes that the general assumption is that such duties "mean those imposed by criminal or public law e.g. aid in investigation of crime or security matters, not as extending to duties under private law, e.g., to help prevent copyright infringement - since that would negate the point of Article 15 and indeed Art 14 generally".[112] Still, the interpretation of the recital raises challenges. In particular, it is difficult in some cases to distinguish statutory-type duties of care from the liability of intermediaries for third party infringement, where the latter is established (as occurs in some national laws) on the basis of negligence.[113]

Examining the history of the ECD may be helpful in this respect, as it may clarify the intention of the legislator. As stated in a letter from Director General of the Internal Market DG to an MEP on this topic, recital 48 only "aims at explaining the content of Article 15 and its implications for Member States", and does not allow the imposition of obligations contrary to the prohibition contained in Article 15:

> *This prohibition [in Article 15] concerns obligations of a general nature and does not concern monitoring obligations in a specific case nor does it affect orders by national authorities in accordance with national legislation, which is explained in recital 47. Furthermore, as explained in recital 48, this prohibition does not concern certain duties of care which can reasonably be expected from service providers and which are specified by national law. Such duties of care could for instance consist in the making available of complaint-systems or in the operation of notice and take down procedures and hot-lines. By contrast, any general obligation to monitor or supervise data which are transmitted or stored will not be possible under the directive, given the clear wording of Article 15 para 1. This was after difficult negotiations eventually accepted by Member States, since given the sheer amount of data which are transmitted or stored any general monitoring obligation would be unreasonable and unrealistic.*[114]

Duties of care may relate to *ex ante* or *ex post* measures. *Ex post* measures regard the removal or disabling of content after obtaining knowledge of the same, as in the context of an NTD system. Such duties follow naturally from the regime of Article 14(1) ECD and, as such, do not appear to be per se problematic. Conversely, *ex ante* measures concern duties of care as obligations on the platform to prevent infringement prior to obtaining knowledge or awareness of the same. Such proactive

[112] Edwards WIPO, p.10, relying also on R Bagshaw, 'Downloading Torts: An English Introduction to On-Line Torts' in Snijders and Weatherill (ed), *E-Commerce Law*, Kluwer, 2003.

[113] Angelopoulos 2016, pp. 94-95; and Angelopoulos 2017, pp. 27-29 (exemplifying with French and German Law).

[114] See European Commission, letter of John F. Mogg to Mrs Cederschild, Brussels 13 June 2000, available at https://www.asktheeu.org/en/request/2250/response/7914/attach/2/letter%20Mogg%20to%20MEP.pdf.

measures are difficult to reconcile with the prohibition to actively to seek facts or circumstances indicating illegal activity in Article 15 ECD.[115]

For this reason, some authors argue for a restrictive interpretation of the scope of such duties. One avenue to do so is by restricting their application to public law, in line with Edwards' view described above. However, this does not seem to have been the intention of the EU legislator, as expressed in the above-quoted letter. Another approach is to limit, the application of duties of care to obligations outside those set forth in Article 14 ECD, concerning the removal and disabling of infringing information.[116] That is to say, hosting providers that comply with Article 14 cannot be held liable in any case for the information stored. Still, Member States may freely impose duties of care on intermediaries regarding other aspects, such as duties of information that concretize the obligations mentioned in Article 15(2) ECD.[117] From a teleological perspective, and resorting to the letter quoted above, arguably, the legislator's intention was somewhat different than these approaches. Namely, what was apparently envisaged were more narrow duties of care that could assist and concretize the concepts of removal and disabling of access to infringing information, predominantly related to *ex post* reactive measures.

LIMITS IMPOSED BY PROHIBITION ON A GENERAL MONITORING OBLIGATION

Article 15 ECD prohibits the imposition by Member States of general obligations to monitor for providers of the types of services covered by the directive's safe harbours. For hosting providers, this means a prohibition to actively to seek facts or circumstances indicating illegal activity for the information they store. The provision does not apply to *voluntary* proactive measures of the type endorsed in the Communication and Recommendation on "tackling illegal content online". Where it does apply, the prohibition limits the potential scope of injunctions and duties of care.

For the most part, Article 15 does not impose significant restrictions on obligations to remove or disable access to unlawful content after an hosting provider obtains knowledge of the same following a sufficiently precise and adequate notification by a third party, i.e. the typical NTD scenario. More problematic in this light are obligations to take proactive measures, such as filtering.

Pursuant to Recital 47 ECD, a distinction is made between "general" and "specific" monitoring obligations, the first being prohibited and the second allowed under Article 15. The Court has provided some guidance as to what constitutes "general", and therefore inadmissible, filtering. Starting with *L'Oréal*, it states that Article 15 bars "active monitoring of all the data of each of [*a platform's*] customers in order to prevent any future infringement of intellectual property rights".[118]

[115] Bagshaw 2003, p. 72; Angelopoulos 2016, pp. 94-95.

[116] Edwards, L. (2005) The problem of intermediary service provider liability. In, Edwards, Lilian (ed.) *The New Legal Framework For E-commerce In Europe.* Oxford, UK. Hart, pp. 114-115; Angelopoulos 2017, p. 14.

[117] Angelopoulos 2016, p. 95.

[118] C-324/09 - *L'Oréal*, par. 139.

The point is developed in *Scarlet Extended* (concerning an access provider) and *Netlog* (an hosting provider), where the Court found that Article 15 prohibits imposing an obligation on a platform to actively monitor "almost all the data relating to all of its service users in order to prevent any future infringement of intellectual-property rights".[119] Importantly, all these cases relate to IPRs, which allowed the Court to additionally rely on the general obligation in the Enforcement Directive that the measures at issue "must be fair, proportionate and not excessively costly".[120]

Still, the Court is yet to clearly delimit the boundaries of "general" and "specific" monitoring obligations, there remaining a significant scope for the latter and for thus potentially admissible injunctions and duties of care in light of Article 15 ECD. In determining that scope, and following the Court's case law on IPRs, the general prohibition in this provision should assist in striking of a fair balance between the fundamental rights at stake in the particular case: those of the hosting provider, its users, and the rights holder or injured party.

A particular point of contention on the application of Article 15 relates to *stay down* obligations or *automatic re-upload filters* as duties of care. The issue is that the imposition of such measures can likely only be achieved by filtering all content in the platform in search of specific previously identified unlawful items, which would translate into a general monitoring obligation.[121] The Recommendation on "tackling Illegal Content Online" endorses the voluntary adoption of such re-upload filters in a unequivocal way only for terrorist content[122], but does not take a position on whether a broader imposition of such obligations by Member States runs afoul of Article 15 ECD. In the copyright field, however, currently proposed versions of Article 13 of the Draft DSM Directive contain an obligation of this type for commercial large-scale online media sharing platforms, subject to requirements of effectiveness and proportionality.[123] Furthermore, in the same field, there is diverging national case law on the topic, including instances where *stay down* measures have been rejected due to conflict with the ban on general monitoring.[124]

In sum, there remains a contested area as to what types of "specific" preventive measures are admissible under Article 15 ECD. This area requires further clarification by the CJEU, which clarification will probably be influenced by the specific filtering technology at stake (namely its

[119] C-360/10 - *Netlog*, par 38. See also C-70/10 - *Scarlet Extended*, par. 40.

[120] Angelopoulos 2017, p. 14, referring to Article 3 Enforcement Directive.

[121] Angelopoulos 2017, p. 27. Contra: Nordemann 2018, p. 17.

[122] European Commission Recommendation 2018, Chapter III. para. 37.

[123] Art 13(4), Proposed DSM Directive, https://www.parlament.gv.at/PAKT/EU/XXVI/EU/01/76/EU_17608/imfname_10800647.pdf

[124] Nordemann 2018, pp. 17-18, with references to case law in Germany, Italy and France. The author argues that the question of compliance with Art. 15 ECD ultimately turns on 'the technical solution used by the provider'.

adequacy, effectiveness, context-awareness and safeguards) and the balancing of fundamental rights on a case-by-case basis.