cerre Centre on Regulation in Europe

REPORT

September 2018

Alexandre de Streel
Miriam Buiten
Martin Peitz

LIABILITY OF ONLINE HOSTING PLATFORMS

SHOULD EXCEPTIONALISM END?

The project, within the framework of which this report has been prepared, has received the financial support of the following CERRE members: Google, Microsoft, Orange, Snap and Vodafone. As provided for in the association's by-laws, it has, however, been prepared in complete academic independence.

info@cerre.eu
www.cerre.eu

Table of contents

About CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

About the authors

Alexandre de Streel is a Joint Academic Director at CERRE, Professor of European law at the University of Namur in Belgium and the Director of the Research Centre for Information, Law and Society (CRIDS, part of Namur Digital Institute). He is also an Assessor at the Belgian Competition Authority, visiting professor at the University of Louvain, and a member of the Advisory Board of the Mannheim Centre for Competition and Innovation (MaCCI). His main areas of research are the regulation and the application of competition policy to the digital economy as well as the legal issues raised by the development of artificial intelligence.

Miriam Buiten is a Junior Professor of Law and Economics at the University of Mannheim. Her research focuses on the legal issues surrounding new technologies and artificial intelligence and the role of consumer policy and competition law in regulating the digital economy. Prior to joining the University of Mannheim, Miriam was affiliated to the Rotterdam Institute of Law and Economics. Miriam has been involved in several policy studies for the European Commission and the Dutch government on topics such as the role of online intermediaries in the e-commerce sector and mechanisms to reduce regulatory burdens.

Martin Peitz is a CERRE Research Fellow and Professor of Economics at the University of Mannheim. He is also a Director of the Mannheim Centre for Competition and Innovation. His research focuses on regulation, industrial organisation and microeconomics. Martin holds a PhD in Economics from the University of Bonn.

Executive summary

This Report is concerned with the **EU liability regime for online hosting platforms** when they provide access to illegal material, content or products. The report analyses whether the liability exemption of the e-commerce Directive is still justified given the growing maturity and economic and societal importance of many online platforms. On the basis of a legal and economic analysis, the Report provides recommendations for improving the EU liability regime.

The **diffusion of illegal material online is a problem of 'many hands'** because many private actors (providers of the material and online platforms) contribute to the problem and several private and public actors (providers and platforms, but also other victims and authorities) may be able to contribute to the solution. Hence, the societal responsibility of a safer Internet can be shared among all those hands. The diffusion of illegal material is also a **problem of many rules** because each actor involved is subject to multiple regulations, on liability or otherwise. For the effective detection and removal of illegal material, it is important that all those rules are consistent and provide the right incentives to both private and public actors. Thus, the liability regime of online hosting platforms is one part of a broader regulatory framework; it is key but not unique.

- ***Should digital exceptionalism end?***

In 2000, when the Internet intermediaries, as they were then called, were in their infancy, the EU legislature adopted the **e-commerce Directive with four main objectives**: (i) share responsibility of a safe Internet between all actors involved, (ii) stimulate the development of Internet intermediaries and the e-commerce sector, (iii) achieve a fair balance between conflicting fundamental rights and (iv) build the digital single market.

On liability, the Directive contains four key, complementary rules:

- An **internal market clause** which implies that Internet platforms are only subject to the legal regime, including the liability rule, of the Member State where they are established;
- **Harmonised conditions to get an exemption from the national liability regime** when illegal material is hosted. In a nutshell, the hosting platform can escape liability when it provides a service of a mere technical, automatic and passive nature which implies that it has neither the knowledge of, nor the control over, the material hosted; moreover, the platform should expeditiously remove illegal material when aware of it and should cooperate with public authorities in detecting and removing illegal material;
- **Prohibition on Member States imposing general monitoring measures** of the material hosted;
- **Encouragement of co- and self-regulation** to implement the rules and principles of the Directive.

However with the growing importance of online platforms**, there are calls to increase their liability, or at least their responsibility, in policing the Internet**. At the European level, this has not resulted in a review of the e-commerce Directive but in a three-pronged policy strategy:

- First, to **adopt or adapt sectoral laws** when a specific problem is identified. The EU legislature adopted two new directives, one to combat sexual abuses in 2011 and another one to combat terrorism content in 2017. In 2016, the Commission proposed to review two existing directives which impact the responsibility of video-sharing platforms and platforms hosting large amounts of copyrighted content;
- Secondly, to provide **more guidance on the implementation of the e-commerce Directive in order to step up efforts in tackling illegal material**: in 2017 the Commission adopted a Communication, followed by a Recommendation in 2018 to improve the detection and the removal of illegal content;
- Thirdly, to **develop effective co- and self-regulation schemes**: in 2011, a CEO Coalition was established, in 2012 an ICT Coalition for Children Online and in 2017 an industry alliance was founded to deal with cases of child sexual abuse; in 2015 an EU Internet Forum was initiated to counter terrorist content; in 2016 a Code of Conduct on countering illegal hate speech was adopted; and in that same year a pre-existing Memorandum of Understanding on the sale of counterfeit goods was updated.

Some of these reforms were useful and effective. Nevertheless, in light of the changing societal and economic importance of online platforms, the **fundamental question is whether the e-commerce Directive itself should be revised.** To answer this question, **this report evaluates the appropriate liability for online platforms based on an economic analysis**. From an economic perspective, liability rules should aim at minimising the total costs of harm that result from activities or transactions; market failures may lead to such harm.

- ***What does economics tell us?***

In the context of online platforms, several well-known sources of market failure may come into play: information asymmetries, market power, and negative externalities may be present in isolation or in combination. Online platforms may want to, and be able to, mitigate some market failures. In particular, they may reduce asymmetric information problems and allow markets to function in a way that could not be sustained in the pre-Internet era. Online platforms may also take measures against negative externalities, insofar as they may suffer short-term economic losses or reputational harm, or based on a sense of public responsibility to intervene.

Determining the efficient level of care for online hosting platforms involves a difficult balancing act. First, one has to consider the **instruments available to online intermediaries to prevent harm, and the social costs of these precautionary measures**. Generally, when monitoring costs for the platforms are low, they may be best placed to remove illegal material and prevent harm. In such cases, platforms may monitor on their own initiative as well, meaning that imposing a duty of care on them should not have a significant impact on their viability.

The legal requirements for liability should also **induce online hosting platforms to monitor and remove illegal material in a diligent manner**. On the one hand, platforms could be encouraged to take proactive, voluntary measures to monitor and remove illegal material. This may warrant a clear 'Good Samaritan' clause exempting liability for voluntary action. On the other hand, the liability rule should discourage platforms from taking down too much content, as this would include legal material. A sanction on systematic over-removal may be appropriate to encourage online intermediaries to improve the quality of their notice-and-takedown systems and further develop automated detection technology.

Secondly, the **type and extent of the harm, as well as the type of harmed party,** may influence the need for liability of online hosting platforms. In cases where harm is serious, and where harm is scattered over a large group of parties, there is a stronger argument for some form of liability for online platforms. Different types of online intermediaries may be vulnerable to different types of harm, depending on the type of content hosted on their platforms, and more generally on their business model.

Thirdly, one has to balance the costs of monitoring and the extent of the harm with the **social benefits that the activities of online hosting platforms provide to society**. Liability for harm caused by the activities of platforms increases the costs of doing business, and may prevent some business models from being commercially viable at all. Moreover, small platforms or new entrants may need to be exempted from some obligations, in order to prevent a situation where the liability rules create a regulatory barrier to entry, harming competition in the market provided that there is a clear threshold for exemption.

Overall, from an economic perspective, there is likely no one-size-fits-all liability rule for all types of platforms and all types of harm. Ideally, the duty of care for online hosting platforms varies depending on several general factors, including the level of precaution costs of the platforms, the possibility for victims to notify or even prevent harm, and the extent of the harm. While, in practice, it may be neither possible nor desirable to impose liability exactly along the lines of economic determinants, these factors for differentiation may inform policy makers as to the appropriate type of duty of care for online hosting platforms.

- ***Our recommendations***

On that basis, we make the following **two sets of recommendations**: the first set is general and deals with the structure of the regulatory framework, while the second is specific and deals with the liability exemption of the online hosting platforms.

1. On the **structure of the regulatory framework**, we suggest that:

- As tackling illegal material online is a problem of many hands and many rules (some dealing with liability, others dealing with establishment and operations), **all these rules need to be consistent with each other and contribute, with their combined incentive effects, to effective detection and removal of illegal material online**;

- The **liability rules**, which are one important part of this regulatory framework, **should efficiently share the burden of policing the Internet among all the private and public actors** involved;
- These **liability rules need to be principle-based** to ensure an easy adaption to rapidly and unpredictably evolving technology and markets; however, to alleviate the drawbacks of legal uncertainty, these rules should be clarified using delegated or implementing acts or interpretative guidance, or supplemented with effective co-/self-regulation schemes.

2. On the **liability of hosting platforms** and more specifically their right to exemption, we suggest:

- **Requiring hosting platforms, in order for them to benefit from the liability exemption, to provide a practical and proportionate infrastructure allowing users to comply with their responsibilities, and ensuring an effective detection and removal of illegal material**. The required features of such infrastructure or system, which may vary according to the type of platforms, could be specified in a Commission legal act (either a delegated act or a Recommendation) and would include most of the characteristics identified by the Commission in its recent Recommendation and Communication on tacking illegal content online. In particular, such systems should (i) allow for effective and transparent notice-and-takedown processes, (ii) rely on appropriate, proportionate and specific proactive monitoring measures, which may be based on automated tools if safeguards are in place, and (iii) ensure that, upon knowledge, illegal material is removed expeditiously in a transparent and fair manner;
- Moreover, for **illegal material that justifies a more extensive duty of care,** the baseline regime of the revised e-commerce Directive should be complemented with **effective co-/self-regulatory schemes**.

1. Introduction

In February 2017, the journal The Economist noted that Internet firms' immunity against potential liability actions for the illegal material carried over their platforms was under threat and that this digital exceptionalism was being eroded. The article concluded that: '*giving platforms a free pass is increasingly difficult for regulators and courts: they simply have become too important for the economy and society more generally. Successful online platforms, in other words, carry the seeds of their own regulation*'.[1] This report explores whether platforms have a free pass today and whether their liability should increase with their economic and societal importance and if so, what is the best way to do so.

1.1. Scope and aim of the report

This report analyses the liability of online platforms for illegal material, being content or product, carried over the platforms. In doing so, the report focuses on specific types of platforms, or more precisely, on specific online services provided. Indeed, the term 'online platform' is a catch-all concept which covers very different services, business models and legal categories. As noted by the Commission, online platforms '*cover a wide-ranging set of activities including online advertising platforms, marketplaces, search engines, social media and creative content outlets, application distribution platforms, communications services, payment systems, and platforms for the collaborative economy*.'[2]

This report focuses on the hosting service, which is defined by EU law as the storage of information provided by the users of the platform.[3] We focus on this type of service because it is currently subject to specific liability exemption, although not given a 'free pass' as hinted by The Economist, and because this type of service faces the strongest call for additional responsibility. Therefore, this report does not deal with the other two types of information society services that benefit from the liability exemption under EU law, namely the mere conduit and the caching services, as their legal regime is less controversial. Moreover, the report deals with liability, and its possible exemption or limitation, when illegal material is hosted. It does not deal with the responsibility or the accountability for hosting material that is harmful but legal.

The report aims to propose policy recommendations for an efficient EU liability regime for hosting service providers. Our recommendations are based on a legal and economic analysis of

[1] The Economist, 'Internet firms' legal immunity is under threat', 11 February 2017, available at https://www.economist.com/business/2017/02/11/internet-firms-legal-immunity-is-under-threat.

[2] Communication of the Commission of 25 May 2016, Online Platform and the Digital Single Market, COM(2016) 288, p. 2. The Commission describes the different business models in its Staff Working Paper of 25 May 2016 on online platforms, SWD(2016) 172.

[3] Art. 14 of the Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ [2000] L 178/1.

the current rules and the incentives they give to market players to reduce illegal material on the Internet.

The report is divided in 4 Chapters: First, this introduction defines the scope and the aims of the report and sketches the main actors involved in the eco-system. Then, Chapter 2 explains the EU legal regime on the hosting intermediaries when they host illegal material. Next, Chapter 3 carries an economic analysis of those liability rules. On that basis, Chapter 4 concludes with policy recommendations to improve the current EU legal regime.

1.2. Complex and evolving eco-system

As explained by Helberger et al. (2018), diffusion of illegal content online is a problem of 'many hands.' This concept '*refers to a situation in which different entities contribute in different ways to a problem, or the solution to a problem, in a manner that makes it difficult to identify who is responsible for which actions and what consequences and on this basis allocate accountability and responsibility accordingly*' (Helberger, 2018:3). Indeed, in case of illegal material online, many private and public entities contribute to the problem, i.e. the diffusion of the illegal material, and may be able to contribute to the solution, i.e. the detection and the removal of such material.

The main private players are: (i) the provider of the material, (ii) the online platform which contributes to the diffusion of the material to a larger audience, (iii) the use of the material, (iv) the victim of the illegality, and (v) possibly other actors which may help the platform and/or the victims to detect the illegality such as trusted flaggers, right enforcement organisations, etc.

Those actors may be very heterogeneous and their characteristics affect their legal obligations and their private incentives to place or remove illegal material:

- The provider of the material may be a professional user or a consumer, the former being subject to more obligations in the B2C relationship than the latter;
- The online platform may be a mere passive hosting platform or play a more active role, the former benefiting from a liability exemption that is not available to the latter;
- The user may be actively searching for illegal material or unaware of the illegality of the content;
- The victims of the illegality may be concentrated, such as right-holders in case of diffusion of copyrighted material without licence or sale of counterfeit goods, or diffused, such as the society at large in case of terrorist content; incentives to launch liability actions are higher for the former than the latter;
- Actors supporting platforms and victims may use automated technologies or merely rely on human checks, the former being less expensive than the latter.

Some of the actors may be victim and user at the same time or, in the case of partial vertical integration, provider and online platform at the same time. Moreover, public authorities may be actors, as they also have important roles to play, beyond rule making, in contributing to the detection of illegal material as well as in forcing the removal of such material.

As the diffusion on illegal material online is a problem of *many hands*, the societal responsibility and the legal liability for a safer Internet is shared among all those hands. Clearly, the providers can be directly liable for posting illegal material online. But often they will be difficult to identify and can be insolvent. In this case, victims will turn to the platforms with a secondary liability action.

Thus the diffusion of illegal material online is also a problem of *many rules*: (i) first the liability rules of the different actors in the digital eco-system, such as the primary liability of the providers of the materials and the secondary liability of the platforms; (ii) second, the other rules which apply to those actors such as consumer protection, data protection, antitrust, product safety, etc. All those rules need to be consistent with each other and give incentives in order to allocate in the most efficient way the responsibility among the many hands on the Internet. This is what we study in the following Chapters.

Of course, there are incentives other than rules which stimulate providers and online platforms to alleviate illegal material such as: (i) direct monetary incentives, especially when there is competition by other platforms as legal content providers may leave a platform that hosts illegal content and consumers may leave a platform that does not protect them from malfunctioning products; and (ii) dynamic considerations, such as the reputation of the platforms or the threat of regulation in case of the presence of illegal material which is deemed as excessive by public authorities. This report focuses on the incentives provided by legal rules, while acknowledging these other incentives.

2. EU Rules on the liability of online intermediaries

This chapter depicts the EU legal regime on the liability of online hosting intermediaries. The first section describes the rules of the e-commerce Directive, adopted at the turn of the century when most online platforms were in their infancy. As those platforms have matured and their economic and societal power increased, they face more pressure to increase their responsibility. The second section then reviews the evolution of the EU liability regime in light of changes to sectoral laws, guidance of the e-commerce directive, and co and self-regulation to tackle particularly harmful illegal materials.

2.1. The 2000 Directive on electronic commerce

The e-commerce Directive (ECD) was proposed by the Commission in 1998 when online intermediaries were in their infancy.[4] The Directive was adopted by the EU legislature in 2000 and, as claimed by the Commission, it '*provides for a technologically neutral framework and the liability regime strikes a balance between the several interests at stake, in particular between the development of intermediary services, the societal interest that illegal information is taken down quickly, and the protection of fundamental rights*.'[5]

The liability rules of the ECD aim to achieve four main objectives:

- First, *share responsibility between all the private actors* of the eco-system in ensuring the minimisation of illegal material and a good cooperation with public authorities. Thus, the victims should notify to the hosting intermediaries any illegality they observe and the intermediaries should remove or block access to any illegal material of which they are aware. This should ensure timely private enforcement that may effectively complement public adjudication. That is also why hosting intermediaries should cooperate closely with administrative and judicial authorities.
- Second, *stimulate the development of e-commerce* by increasing legal certainty on the role of each actor in the value chain[6] and by ensuring that the hosting intermediaries do not have an obligation to monitor the legality of all material they store. This would have been extremely expensive, especially at a time when machine-learning based technologies were absent or very nascent, or even impossible when the determination of the illegality is contextual.

[4] Explanatory Memorandum of the Commission proposal for a directive on certain legal aspects of electronic commerce in the internal market, COM(1998) 586, p. 6.
[5] Commission Staff Working Document of 11 January 2012 on online services, including e-commerce, in the Single Market, SEC(2011) 1641, p. 24. The recital 41 ECD notes that: '*this Directive strikes a balance between the different interests at stake (…)'.*
[6] Explanatory Memorandum of ECD, COM(1998) 586, p. 8.

- Third, *achieve a fair balance between conflicting fundamental rights*: (i) respect for privacy and the protection of personal data guaranteed by Articles 7 and 8 of the Charter of Fundamental rights of the EU; (ii) freedom of expression and information protected by Article 11 of the Charter; (iii) freedom to conduct business guaranteed by Article 16 of the Charter; and (iv) right to property, including intellectual property, protected by Article 17 of the Charter.[7]
- Fourth, *build the digital single market* by adopting a common EU standard for liability exemption, especially at a time when national rules and case-laws were increasingly divergent.[8]

The Directive on electronic commerce applies to the providers of all types of information society service which is defined as '*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*'.[9] This is a broad category but not unlimited, as the Court of Justice decided in the different Uber cases.[10] In particular, in the *Uber France* case, the Court decided that:

> *21. the Court found that the **intermediation service provided by (Uber) was inherently linked to the offer by that company of non-public urban transport services**, in view of the fact that, in the first place, that company provided an application without which those drivers would not have been led to provide transport services, and the persons who wished to make an urban journey would not have used the services provided by those drivers and, in the second place, that company exercised decisive influence over the conditions under which services were provided by those drivers, inter alia by determining the maximum fare, by collecting that fare from the customer before paying part of it to the non-professional driver of the vehicle, and by exercising a certain control over the quality of the vehicles, the drivers and their conduct, which could, in some circumstances, result in their exclusion (…)*
>
> *22. The Court found, on the basis of those factors, that the **intermediation service at issue in that case had to be regarded as forming an integral part of an overall service the main component of which was a transport service** and, accordingly, had to be classified, not as an 'information society service'*

Thus, if an online intermediation service is provided only as an accessory of another service, the qualification of the online intermediation is absorbed by the qualification of the service for which the intermediation is the accessory. In this case, the online intermediation service provided by Uber has been qualified as a transport service.

[7] Explanatory Memorandum of ECD, COM(1998) 586, p. 16. See also the Report of the Special Rapporteur of the United Nation of 6 April 2018 on the promotion and protection of the right to freedom of opinion and expression.
[8] Explanatory Memorandum of ECD, COM(1998) 586, p. 8.
[9] Art. 1(b) of the Directive 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, OJ [2015] L 241/1.
[10] Case C-434-15 *Uber Spain*, ECLI:EU:C:2017:981 and Case C-320/16 *Uber France*, ECLI:EU:C:2018:221.

The e-commerce Directive regulates the establishment of the providers of information society services, the information to be given to the users, the contracts concluded by electronic means and the liability exemptions of the providers of three types of information society services: the mere conduit, the caching and the hosting providers.

As already explained, this report focuses only on the liability of hosting providers. In that regard, the e-commerce Directive contains four complementary rules: an internal market clause, harmonised conditions for liability exemption, prohibition of the imposition of general monitoring, and encouragement of co- and self-regulation.

2.1.1. The Internal market clause

Article 3 of the ECD contains the so-called internal market clause, which establishes that a provider of information society services is only subject to the rules - including the rules on liability - of the Member State where it is established. It may then provide the services across the 27 other Member States without being subject to the rules of those other States. Unless there are exceptional circumstances related to public policy, health, security or protection of consumers and investors,[11] Member States may not restrict the freedom to provide information society services from another Member State.

2.1.2. Harmonised conditions for liability privilege

(a) The rules

Article 14 ECD applies to the provider of a specific type of information society service, the hosting service that consists in the storage of information provided by a recipient of the service. Article 14 ECD harmonises the conditions under which the provider of such hosting service may escape the national liability rule of the country where it is established for the illegal material it hosts. According to the ECD:

> *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.*

[11] This safeguard clause has been very rarely used by the Member States: Commission Staff Working Document of 11 January 2012 on online services, including e-commerce, in the Single Market, SEC(2011) 1641, p. 21.

> *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* (emphasis by the authors).

Thus, an online intermediary hosting illegal material escapes national liability rules if it does not know the illegality or, when it knows, it acts expeditiously to remove or block access to the material. The procedure for the intermediary to be informed and to act, the so-called notice-and-takedown process, is not described in the directive but can be defined at the national level.[12] Moreover, the hosting providers should cooperate with administrative and judicial authorities requiring the removal of illegal material.

Article 14 ECD only harmonises at the EU level the conditions to benefit from the liability exemption but does not harmonise the liability conditions themselves, which remain governed by the national substantive and procedural rules. The exemption is *horizontal* and covers all types of illegal material, be it terrorism content, hate speech, counterfeit product, copyrighted content or otherwise. The exemption is also *functional* and applies to categories of services (the hosting information society service) but not to categories of online providers. Thus the fact that a provider qualifies for an exemption from liability as regards a particular act does not provide it with an exemption for all its other activities.[13]

(b) Difficulties in interpreting the rules

Article 14 ECD raises a series of difficult interpretative legal questions in relation to the definition of the hosting services and the material conditions necessary to get the exemption, in particular, the concepts of actual knowledge and expeditious removal/blocking.[14]

Regarding the scope of hosting services,[15] the Court of Justice, in *Google France v. Vuitton*, has judged that:[16]

> *113. In that regard, it follows from recital 42 in the preamble to Directive 2000/31 that the exemptions from liability established in that the directive cover only cases in which the activity of the information society service provider is 'of a* ***mere technical, automatic and passive nature****', which implies that that service provider 'has* ***neither knowledge of nor control over the information*** *which is transmitted or stored'*

[12] In 2011, most of the notice-and-take down procedures enacted at the national level concern mere conduit services (Commission Staff Working Document on online services in the Single Market, SEC(2011) 1641, p. 42). Since then, several Member States (Finland, France, Hungary, Lithuania, UK, Spain and Sweden) have enacted in their national legislations notice-and-takedown procedures applicable to hosting services: Commission Staff Working Document on Mid-term review of DSM Strategy, SWD(2017) 155, p. 27.
[13] See Commission Explanatory Memorandum of the proposed directive, COM(1998), 586, p. 27.
[14] See Commission Staff Working Document on online services in the Single Market, SWD(2011) 1641, pp. 26-47.
[15] On this issue, see Leonard (2012), Nordemann (2018:9-11) and Van Eecke (2011:1468-1474).
[16] Cases C-236/08 to C-238/08 *Google France v Louis Vuitton*, ECLI:EU:C:2010:159. Also more recently, Case C-484/14 *Mc Fadden*, ECLI:EU:C:2016:689, para 62.

> *114. Accordingly, in order to establish whether the liability of a referencing service provider may be limited under Article 14 of Directive 2000/31, it is necessary to examine whether the* ***role played by that service provider is neutral****, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores* (emphasis by the authors).

Then in *L'Oreal v. eBay*, the Court of Justice clarified further that: [17]

> *115. (…) the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and* ***provides general information to its customers cannot have the effect of denying it the exemptions*** *from liability provided for by Directive 2000/31 (…).*
>
> *116. Where, by contrast, the operator has* ***provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers****, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have* ***played an active role*** *of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31* (emphasis by the authors).

There is thus a very fine line between, on the one hand, services that are purely passive, neutral, without knowledge[18] and can benefit from the liability exemption and, on the other hand, services that are move active and cannot benefit from the exemption.[19]

The other difficult issue is the level of knowledge leading to losing of the exemption when the provider is not acting expeditiously.[20] In *L'Oreal v. eBay*,[21] the Court of Justice judged that:

> *120. (…) it is sufficient, in order for the provider of an information society service to be denied entitlement to the exemption from liability provided for in Article 14 of Directive 2000/31, for it to have been* ***aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality*** *in question and acted (…)*
>
> *122. The situations thus covered include, in particular, that in which the operator of an online marketplace uncovers,* ***as the result of an investigation undertaken on its own initiative****, an illegal activity or illegal information, as well as a situation in which the operator is* ***notified of the existence of such an activity*** *or such information. In the second case, although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of*

[17] Case C-324/09, *L'Oreal et al. v. eBay*, ECLI:EU:C:2011:474, points 115-116. In Case 291/13, *Papasavas,* ECLI:EU:C:2014:2209, point 45, the Court judged that: *'(…) since a newspaper publishing company which posts an online version of a newspaper on its website has, in principle, knowledge about the information which it posts and exercises control over that information, it cannot be considered to be an 'intermediary service provider' within the meaning of Articles 12 to 14 of Directive 2000/31, whether or not access to that website is free of charge.'*

[18] According to Montero (2011) and Van Eecke (2011:1483), the criterion of knowledge is more relevant for hosting services than the criterion of passivity or neutrality that are better adapted to the mere conduit and caching services.

[19] For an overview of the national case-law which is not always consistent across the Member States, see Van Eecke (2011:1469-1472).

[20] On this issue, see Nordemann (2018:11-13), Van Eecke (2011:1475-1480).

[21] Case C-324/09, *L'Oreal et al. v. eBay.* For the different national interpretations given to the knowledge condition, see Commission Staff Working Document on online services in the Single Market, SWD(2011) 1641, pp. 33-36.

Directive 2000/31, given that notifications of allegedly illegal activities or information ***may turn out to be insufficiently precise or inadequately substantiated****, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality* (emphasis by the authors).

The Court of Justice thus interprets the ECD with common sense and relies on the standard of a diligent provider to determine whether the level of knowledge would lead to losing the exemption when not followed with action.[22]

A related issue is whether Article 14 dis-incentivises the hosting intermediaries to proactively monitor the legality of the material they host because, if they would do so, they may lose the benefit of the liability exemption. This is sometimes referred to as the 'Good Samaritan paradox'.[23] During the successive Commission public consultations, hosting intermediaries have mentioned this legal risk of voluntary introducing more proactive measures.[24] However, in its Communication of September 2017 on tacking online content (analysed below), the Commission considers that voluntary proactive measures '*do not in and of themselves lead to a loss of the liability exemption, in particular, the taking of such measures need not imply that the online platform concerned plays an active role which would no longer allow it to benefit from that exemption*. '[25] This is also the view of Nordemann (2018:10) citing a case from the Court of Appeal of Hamburg having found that the use by YouTube of its Content ID filtering system does not imply that YouTube offers an active service and loses the benefit of liability privilege.[26]

[22] On that point, Nordermann (2018:12) suggests that the ECD should not be interpreted as allowing the liability exemption only until the hosting platform has an actual knowledge of the specific infringement committed. According to this author, a standard knowledge should suffice in particular when hosting platforms are running business model fostering illegal material.

[23] Nordemann (2018:10), Van Eecke (2011). Note that the US law provides explicitly for a Good Samaritan clause, hence does not carry this dis-incentive against voluntary proactive measures: Section 230(c) of the US Communication Decency Act states that: '(…) *No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable* (…)'

[24] For the 2011 consultation, see Commission Staff Working Document on online services in the Single Market, SEC(2011) 1641, p. 35 which also mentions a judgment from the Hamburg regional court where an ISP that had voluntarily implemented a flagging system (that enables users to put red flags next to content they considered to be potentially illegal) was considered to have actual knowledge of illegal content because of this very flagging system it had voluntarily introduced (*Gisele Spiegel v. YouTube LLC).* For the 2015-2016 consultation, see Communication on Online Platforms, COM(2016) 288, p. 9 and Staff Woking Document of the Commission of 10 May 2017 on the Mid-Term Review on the implementation of Digital Single Market Strategy, SWD(2017) 155, p. 28.

[25] COM(2017) 555, p. 13.

[26] Hamburg Oberlandesgericht, 1 July 2015, 5 U 87/12 juris para. 198: '*In light of this, the fact that the (YouTube) continuously checks its stock of videos using content-ID processes and in certain cases blocks them cannot be used against it. This is because those checks are, firstly, also a measure which (YouTube) does not undertake solely in its own business interest but which (YouTube) uses to meet its legal responsibility so that the content recognised as rights infringing no longer remains available to the public (…) That type of knowledge cannot, by its very nature, lead outside the scope of Article 14 e-commerce Directive because otherwise any type of prevention or removal would inherently be impossible for the service provider because the provider would not be allowed to obtain knowledge of the information*

2.1.3. The prohibition of the imposition of general monitoring and injunction

(a) The rules

Article 15 ECD prohibits the Member States from imposing on the providers of hosting services a general monitoring obligation to detect illegal material. According to the ECD:

> *1. Member States shall **not impose a general obligation** on providers, when providing the services covered by Articles 12, 13 and 14, to **monitor** the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.*
>
> *2. Member States **may establish obligations** for information society service providers **promptly to inform the competent public authorities of alleged illegal activities** undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements* (emphasis by the authors).

Thus, national administrative or judicial authorities may not impose, with injunction or otherwise, a general monitoring obligation. However, they may impose specific monitoring obligations. Moreover, Article 15 ECD only deals with monitoring measures that are imposed by authorities but not voluntary measures that are taken on the initiative of hosting intermediaries. In addition, as for Article 14, Article 15 ECD foresees cooperation between the providers of hosting services and the administrative and judicial authorities.

(b) Difficulties in interpreting the rules

Article 15 ECD raises several difficult interpretative legal issues,[27] in particular the frontiers between the imposition of general monitoring measures - which is prohibited - and the imposition of specific monitoring measures - which is allowed. This issue is particularly complex when Article 15 ECD needs to be combined with other EU rules allowing holders of intellectual property rights to apply for an injunction against intermediaries whose services are used to infringe their IP rights.[28]

In *SABAM v. Netlog*, the Court of Justice decided that the combination of Article 15 ECD and the IP legislations preclude:[29]

> *a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering information which is stored on its servers by its service users; which*

---

hosted on its service, without jeopardising its status as hosting provider. Such a consequence cannot have been intended by the legislature.'

[27] See Commission Staff Working Document on online services in the Single Market, SWD(2011) 1641, pp. 47-51.

[28] For copyright, see Article 8(3) of Directive 2001/29 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, OJ [2001] L 167/10; for other intellectual property rights, see Article 11 of Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ [2004] L 195/16.

[29] Case C-360/10 *SABAM v. Netlog,* ECLI:EU:C:2012:85. Also Case C-70/10 *Scarlet Extended v. SABAM*, ECLI:EU:C:2011:771.

applies indiscriminately to all of those users, as a preventative measure, exclusively at its expense, and for an unlimited period; which is capable of identifying electronic files containing musical, cinematographic or audiovisual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright.

Later in *UPC Telekabel*, the Court of Justice explained further that injunction needs to achieve a fair balance between different fundamental rights protected by the Charter on Fundamental rights of the EU:[30]

> *47. (…) it must be observed that an injunction (…) makes it necessary to **strike a balance**, primarily, between (i) copyrights and related rights, which are **intellectual property** and are therefore protected under Article 17(2) of the Charter, (ii) the **freedom to conduct a business**, which economic agents such as internet service providers enjoy under Article 16 of the Charter, and (iii) the **freedom of information** of internet users, whose protection is ensured by Article 11 of the Charter* (emphasis by the authors).

In this case, the Court then judged that a fair balance between those rights can be found when:[31]

> *63. (…) they do **not unnecessarily deprive internet users of the possibility of lawfully accessing** the information available and that they have the **effect of preventing unauthorised access** to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right* (emphasis by the authors).

However, the Court of Justice never traced a clear line between prohibited general monitoring measures and allowed specific monitoring measures and, consequently, judgments by national courts diverge on this issue.

2.1.4. The encouragement of co and self-regulation

Finally, Article 16 ECD encourages the establishment and the monitoring of codes of conduct at the EU and national levels to contribute to the proper implementation of the rules of the ECD.[32] Article 16 ECD mentions the importance of involving consumers in the drafting of these codes of conduct to ensure that the rules remain balanced. It also mentions the necessity to monitor, in cooperation with Member States and the Commission, the implementation of the codes to ensure the effectiveness of the rules.

---

[30] Case C-31412 *UPC Telekabel Wien*, ECLI:EU:C:2014:192. Also previously, Case C-324/09 *L'Oréal,* para 143. On the balancing of fundamental rights, see also Report of the Special Rapporteur of the United Nation of 6 April 2018 on the promotion and protection of the right to freedom of opinion and expression.

[31] *Ibidem*, also more recently, Case C-484/14 *Mc Fadden*, para 96.

[32] Article 17 of the IP Enforcement Directive 2004/38 also encourages the adoption and the monitoring of Codes of conduct at the EU level.

As explained below, this provision has led to an increasing reliance on co- and self-regulation to tackle certain types of illegal materials which are particularly harmful, such as child abuse content, terrorism content, hate speech or counterfeit goods.

2.2. Evolution of the EU regulatory framework

Since the adoption of the e-commerce Directive in 2000 when the Internet intermediaries were still in their infancy, technology and markets have changed dramatically.[33]

First, online platforms - as they are now called - are offering new types of services with the development of web 2.0 relying on user-generated content or the collaborative economy involving prosumers. Hence, the users, but also the platforms, play a more active role. For these new services, it may be more difficult to apply the criteria set by the Court of Justice to define the hosting services – namely a mere technical, automatic and passive role which implies that that service provider has neither knowledge of nor control over the information which is stored.[34]

Second, some online platforms have become large. This is often attributed to important direct and indirect network effects, which can be partly due to data-driven feedback loops.[35] This scale has several consequences: (i) those platforms may have more financial, technological and human capacity to prevent and remove illegal material than the Internet intermediaries at the turn of the century, and (ii) given the prevalence of those platforms, the harm generated by illegal material can be more massive than when the ecommerce Directive was adopted.

Third, with the rapid progress of artificial intelligence, new effective machine-learning based techniques are available for identifying illegal content.[36] This, in turn, decreases the costs for victims and online intermediaries to prevent harms caused by the illegal material.

Thus today, 20 years after the Commission proposed the e-commerce Directive, the EU institutions recognise that online platforms play a very important economic and societal role which should bring wider responsibility.[37]

This has led some Member States to adopt specific legislations to increase the liability, or at least the responsibility and the accountability, of some online platforms at the risk of

[33] See also Sartor (2017:19-23).
[34] Montero (2011); Van Eecke (2011).
[35] Belleflamme and Peitz (2015); Martens (2016).
[36] For an overview of those techniques to detected copyrighted material, see Annex 12 of the Commission Impact Assessment on the Copyright Proposal, SWD(2016) 301.
[37] Communication from the Commission of 25 May 2016 on online platforms and the Digital Single Market, COM(2016) 288; European Parliament Resolution of 15 June 2017 on online platforms and the digital single market. For online terrorist content, the Conclusions of the European Council of 22-23 June 2017 notes at para 2: '*Industry has its own responsibility to help combat terrorism and crime online. Building on the work of the EU Internet Forum, the European Council expects industry to establish an Industry Forum and to develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures at EU level, if necessary (…)*.'

undermining the digital single market. This has also led the Courts of some Member States to interpret the national provisions transposing the e-commerce Directive in a more restrictive way,[38] possibly increasing the divergences across national case-law, which may also undermine the digital single market and legal certainty.[39]

The increasing importance of online platforms and the new risks of digital single market fragmentation have led the Commission to pursue a three-pronged strategy: (i) adapt sectoral hard-law when there is a specific problem; (ii) give more guidance on the interpretation of the controversial provisions of the e-commerce Directive, in particular regarding the notice-and-takedown and the reliance on voluntary proactive measures; and (iii) encourage coordinated EU-wide co and self-regulation for the illegal materials which are particularly harmful.[40]

2.2.1. Adapting the sectoral hard-law

Since 2010, several EU laws have been adopted or adapted to increase the role of online intermediaries in fighting some illegal material. In 2011, the EU legislature adopted a Directive on child sexual abuses that provides for obligations against websites containing or disseminating child sexual abuses:[41]

> *1. Member States shall take the necessary measures to ensure the **prompt removal of web pages** containing or disseminating **child pornography** hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.*
>
> *2. Member States may take measures to **block access** to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by **transparent procedures and provide adequate safeguards**, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress* (emphasis by the authors).

In 2017, the EU legislature adopted a Directive on terrorism that provides for obligations against public provocation online to commit a terrorist offence:[42]

> *1. Member States shall take the necessary measures to ensure the **prompt removal of online content** constituting **a public provocation to commit a terrorist offence**, as referred to in Article 5 that is hosted in their territory. They shall also endeavour to obtain the removal of such content hosted outside their territory.*

[38] See Kohl (2013).
[39] Commission Staff Working Document on Mid-term review of DSM Strategy, SWD(2017) 155, pp. 28-29; Commission on Tackling Illegal content, COM(2017) 555, p. 5.
[40] Communication on online platforms, COM(2016) 288, p. 9.
[41] Article 25 of the Directive 2011/92 of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, *O.J.* [2011] L 335/1.
[42] Article 21 of the Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, *O.J.* [2017] L 88/6.

2. Member States may, when removal of the content referred to in paragraph 1 at its source is not feasible, take measures to ***block access*** *to such content towards the internet users within their territory.*

3. Measures of removal and blocking must be set following ***transparent procedures and provide adequate safeguards****, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress* (emphasis by the authors).

Thus, those two directives instruct the national authorities of the Member States to limit the diffusion of online content which are particularly harmful and ensure that, in doing so, they are transparent and respect the human rights at stake.

In 2018, the EU legislature agreed on a revision of the Audiovisual Media Service Directive, which includes new obligations for video sharing platforms to tackle hate speech and violence:[43]

1. Without prejudice to Articles 12 to 15 of Directive 2000/31/EC, Member States shall ensure that ***video-sharing platform providers*** *under their jurisdiction* ***take appropriate measures*** *to protect:*

(a) ***minors*** *from programmes, user-generated videos and audiovisual commercial communications which may* ***impair their physical, mental or moral development*** *in accordance with Article 6a(1);*

(b) the ***general public*** *from programmes, user-generated videos and audiovisual commercial communications containing* ***incitement to violence or hatred*** *directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter of the Fundamental Rights of the European Union;*

(ba) the ***general public*** *from programmes, user-generated videos and audiovisual commercial communications containing content the dissemination of which constitutes an activity which is a* ***criminal offence under Union law****, namely public provocation to commit a* ***terrorist*** *offence within the meaning of Article 5 of Directive (EU) 2017/541, offences concerning* ***child pornography*** *within the meaning of Article 5(4) of Directive 2011/93/EU and offences concerning* ***racism and xenophobia*** *within the meaning of Article 1 of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law. (…)*

2. For the purposes of paragraphs 1 and 1a, the ***appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests*** *at stake, including those of the video-sharing platform providers and the users having created and/or uploaded the content as well as the public interest.*

Such measures shall be applied to all video-sharing platform providers. The measures shall be ***practicable and proportionate, taking into account the size of the video-sharing platform service***

[43] Article 28a of the forthcoming Directive of the European Parliament and of the Council amending Directive 2010/13 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, available at http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CULT/DV/2018/07-11/AVMS_Agreedtext_EN.pdf.

***and the nature of the service that is provided**. They shall **not lead to any ex-ante control measures** or upload-filtering of content, which do not comply with Article 15 of Directive 2000/31/EC. For the purposes of the protection of minors, provided for in point (a) of paragraph 1, the most harmful content shall be subject to the strictest access control measures.*

Those measures shall consist of, as appropriate:

*a) including and applying in the **terms and conditions** of the video-sharing platform services the requirements as referred to in paragraph 1;*

(aa) including and applying, in the terms and conditions of the video-sharing platform services, the requirements set out in Article 9(1) for audiovisual commercial communications that are not marketed, sold or arranged by the video-sharing platform providers;

(aaa) having a functionality for users who upload user-generated videos to declare whether such videos contain audiovisual commercial communications as far as they know or can be reasonably expected to know;

*(b) establishing and operating **transparent and user-friendly mechanisms for users** of video-sharing platforms **to report or flag** to the video-sharing platform provider concerned the content referred to in paragraph 1 provided on its platform;*

*(ba) establishing and operating systems through which providers of video-sharing platforms explain to users of video-sharing platforms **what effect has been given to the reporting and flagging** referred to in point (b);*

(c) establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors;

(d) establishing and operating easy-to-use systems allowing users of video-sharing platforms to rate the content referred to in paragraph 1;

(e) providing for parental control systems that are under the control of the end-user with respect to content which may impair the physical, mental or moral development of minors;

*(f) establishing and operating **transparent, easy-to-use and effective procedures for the handling and resolution of complaints** between the video-sharing platform provider and its users in relation to the implementation of the measures referred to in points (b) to e);*

(fa) providing for effective media literacy measures and tools and raising users' awareness of these measures and tools.

Personal data of minors collected or otherwise generated by video-sharing platform providers pursuant to points c) and e) shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

*3. For the purposes of the implementation of the measures referred to in paragraphs 1 and 2, Member States shall encourage the use of **co-regulation** as provided for in Article 4a(1).*

4. Member States shall establish the necessary mechanisms to assess the appropriateness of the measures, referred to in paragraph 2 taken by video-sharing platform providers. Member States

*shall entrust the **assessment of those measures to the national regulatory authorities** and/or bodies.*

5. Member States may impose on video-sharing platform providers measures that are more detailed or stricter than the measures referred to in paragraph 2. When adopting such measures, Member States shall comply with the requirements set out by applicable Union law, such as those set in Articles 12 to 15 of Directive 2000/31/EC or Article 25 of Directive 2011/93/EU.

*6. Member States shall ensure that **out-of-court redress mechanisms** are available for the settlement of disputes between users and video-sharing platform providers relating to the application of paragraphs 1 and 2. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law.*

*6a. Member States shall ensure that users can **defend their rights before a court** in relation to video-sharing platform providers pursuant to paragraphs 1 and 2.*

*7. The Commission shall encourage video-sharing platform providers to **exchange best practices** on co-regulatory codes of conduct referred to in paragraph 3.*

*8. Member States and the Commission may foster **self-regulation** through Union codes of conduct referred to in Article 4a(2)* (emphasis by the authors).

Thus this Directive imposes on some online platforms the adoption of measures against some types of particularly harmful content prohibited by EU law (terrorism content, child pornography and racism and xenophobia) as well as hate speech. Those measures should be proportionate to, on the one hand, the harm that may be caused and, other hand, the capacity of the platform to prevent such harm. They may be based on proactive measures or notice-and-take down and should ensure a fair balance between the fundamental rights at stake.

Finally in 2016, the Commission proposed a new Directive on Copyright in the Digital Single Market, which creates new obligations for platforms hosting large amount of content:[44]

*1. Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with right holders, take **measures to ensure the functioning of agreements concluded with right holders for the use of their works** or other subject-matter or to prevent the availability on their services of works or other subject-matter identified by right holders through the cooperation with the service providers. Those **measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate**. The service providers shall provide right holders with **adequate information** on the functioning and the deployment of the measures, as well as, when relevant, adequate reporting on the recognition and use of the works and other subject-matter.*

*2. Member States shall ensure that the service providers referred to in paragraph 1 put in place **complaints and redress mechanisms** that are available to users in case of disputes over the application of the measures referred to in paragraph 1.*

[44] Article 13 of the Commission Proposal of 14 September 2016 for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016) 593. This directive is still being negotiated between the European Parliament and the Council and the Article 13 is one of the main controversial provision.

3. Member States shall facilitate, where appropriate, the ***cooperation between the information society service providers and right holders*** *through stakeholder dialogues to define best practices, such as appropriate and proportionate content recognition technologies, taking into account, among others, the nature of the services, the availability of the technologies and their effectiveness in light of technological developments* (emphasis by the authors).

2.2.2. Providing guidance on the e-commerce Directive

The second prong of the Commission strategy is to give more guidance on the provisions of the e-commerce directive which are particularly useful to tackle illegal material and which have led to divergent interpretations across national Courts. The Commission adopted a Communication in September 2017 and, six months later, a Recommendation.[45]

(a) Communication of the Commission of Sept 2017 on tackling illegal content online

In September 2017, the Commission adopted a Communication to provide guidance and principles, in line with the e-commerce Directive, to online platforms to step up the fight against illegal content online. [46] The Communication deals with the detection, the removal and the prevention of re-appearance of illegal content.

Illegal content can be detected thanks to public authorities and Courts, users or the platforms themselves when monitoring their traffic. The Communication encourages each of those channels by reminding the platforms of their obligations to cooperate with public authorities and courts, encouraging the platforms to facilitate notices by users in particular by trusted flaggers, and clarifying that the reliance on voluntary proactive measures do not imply that the online platform plays an active role leading them to lose the benefit of liability exemption (in other words, there is good Samaritan paradox in EU law).

Once illegal content has been identified, the platforms should remove it. The Communication reminds the platforms that they should act expeditiously which, in practice, depends on the type of illegal content, the accuracy of the notice and the potential damage caused. Platforms should also enhance transparency on their content policy and their notice-and-takedown procedures. They should also allow counter-notice to alleviate over-removal and abuse of the system.

Finally, on the prevention of re-appearance of illegal content, the so-called stay-down problem, the Communication encourages platforms to take measures which dissuade users from repeatedly uploading illegal content of the same nature and to develop and use automated technologies in that regard.

[45] In 2016, the Commission services have also adapted Guidance on the Unfair Commercial Practice Directive with a specific section on the online sector: Commission Staff Working Document of 25 May 2016 on Guidance on the implementation/application of the Directive 2005/29 on Unfair commercial practices, SWD(2016) 163.
[46] Communication of the Commission of 28 September 2017, Tackling illegal content online. Towards an enhanced responsibility for online platforms, COM (2017) 555.

(b) Recommendation of March 2018 on tackling illegal content online

In March 2018, the Commission adopted a Recommendation setting principles for the providers of hosting services and Member States to take effective, appropriate and proportionate measures to tackle illegal content online. [47] Although Recommendations do not have binding force,[48] they legally carry weight, in particular when they interpret EU law. According to the Commission, the Recommendation *'follows-up on the Communication [of September 2017], reflecting the level of ambition set out therein and giving effect thereto, while taking due account of and building on the important progress made through those voluntary arrangements*.'[49]

The Recommendation sets out the general principles for all types of illegal content, complemented by stricter principles for terrorist content because this material is particularly harmful. The structure of the Recommendation is slightly different from the structure of the Communication because it deals first with notice-and-take down procedures, then with proactive measures and finally with the cooperation between hosting providers and public authorities, trusted flaggers and other hosting service providers.

Regarding the notice-and-take down, the Recommendation calls for procedures that are (i) effective, sufficiently precise and adequately substantiated, (ii) respect the rights of content providers with possibilities of counter-notices and out-of-court dispute settlement and (iii) are transparent.[50]

Regarding proactive measures, the Recommendation encourages appropriate, proportionate and specific measures, which could involve the use of automated means, provided some safeguards be in place, in particular human oversight and verification.[51]

Regarding cooperation, the Recommendation encourages close cooperation between, on the one hand, the hosting services providers and, on the other hand, the judicial and administrative authorities of the Member States, the trusted flaggers (having the necessary expertise and determined on clear and objective basis) and other hosting providers in particular smaller ones which may have less capacity to tackle illegal content.[52]

2.2.3. Stimulating EU co and self-regulation for some illegal material

The last prong of the Commission strategy is to stimulate EU-wide co and self-regulation for illegal materials which are particularly harmful. This has led to several initiatives regarding terrorism content, hate speech, child sexual abuse and counterfeit goods. These experiences

[47] Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ [2018] L 63/50.
[48] Art. 288 TFEU.
[49] Recital 6 of the Recommendation 2018/334.
[50] Points 5-17 of the Recommendation 2018/334.
[51] Points 16-21 of the Recommendation 2018/334.
[52] Points 22-28 of the Recommendation 2018/334.

show that co- and self-regulation can be effective when the rules are agreed by a wide variety of stakeholders representing the main diverging interests at stake and when the implementation of those rules is closely monitored in cooperation with the public authorities.[53] Also, co and self-regulation is particularly effective when concluded in the shadow (under the threat) of regulation.

(a) Fighting against child sexual abuse and child sexual exploitation

In its European Strategy for a Better Internet for Children,[54] the Commission called on the EU institutions, the Member States and the industry to speed up identification of child sexual abuse material disseminated through various online channels, the notification and the takedown of this material and encouraged the strengthening of international cooperation in that regard.

In December 2011, a CEO Coalition to Make the Internet a Better place for Kids was launched with several objectives including the effective takedown of child abuse material.[55] In that regard, the coalition worked to give increased transparency regarding takedown procedures and share best practices. It also worked with Hotlines and law enforcement agencies to improve takedown times.[56] Interestingly, the coalition noted that: '*a one-size-fits-all proposal inhibits member companies from developing and implementing solutions consistent with their business models that will have a demonstrable impact on the successful notification and takedown of child sex abuse* material.' [57]

In 2012, the ICT Coalition for Children Online[58] was set up to deal with both illegal child sexual abuse material and inappropriate content. This was the first initiative of its kind to bring together companies from across the value chain to develop a set of high-level principles which would apply to all members, according to their role and type of business. On illegal child sexual abuse material, members pledge to work closely with law enforcement and to ensure prompt removal of any content found to be illegal, and to provide appropriate links (in the most relevant areas of the service) to allow users to report content which they may believe to be illegal, as well as to obtain appropriate advice and support. They also commit to: providing a clear and simple process whereby users can report content or behaviour which breaches the service's terms and conditions: implementing appropriate procedures for reviewing user reports about images, videos, text and other content or behaviour: providing clear information to users on all

[53] Communication on tackling Illegal Content Online, COM(2017) 555, p.4.
[54] Communication from the Commission of 2 May 2012, European Strategy for a Better Internet for Children, COM(2012) 196.
[55] See https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids. The signatory companies were: Apple, BSkyB, BT, Dailymotion, Deutsche Telekom, Facebook, France Telecom - Orange, Google, Hyves, KPN, Liberty Global, LG Electronics, Mediaset, Microsoft, Netlog, Nintendo, Nokia, Opera Software, Research In Motion, RTL Group, Samsung, Skyrock, Stardoll, Sulake, Telefonica, TeliaSonera, Telecom Italia, Telenor Group, Tuenti, Vivendi and Vodafone.
[56] Summary report of the CEO Coalition working groups, available at https://ec.europa.eu/digital-single-market/node/61973.
[57] *Ibidem*.
[58] http://www.ictcoalition.eu

available report and review procedures; and ensuring that moderators who review user reports are properly trained to determine or escalate content or behaviour presented to them. Members of the ICT Coalition include social networks, video platform providers, mobile operators and ISPs, content providers and others. The Coalition meets twice-yearly in a Stakeholder Forum to exchange information on new developments and members report every two years on their progress in implementing policies to improve the safety of children online.

In February 2017, the Alliance to Better Protect Minors Online, a multi-stakeholder forum facilitated by the Commission, was set up in order to address emerging risks that minors face online, such as harmful content (e.g. violent or sexually exploitative content), harmful conduct (e.g. cyberbullying) and harmful contact (e.g. sexual extortion).[59] It is composed of actors from the entire value chain (devices manufacturers, telecoms, media and online services used by children) [60] Its action plan includes the provision of accessible and robust tools that are easy to use and to provide feedback and notification as appropriate, the promotion of content classification when and where appropriate and the strengthening of the cooperation between the members of the Alliance and other parties (such as Child Safety Organisations, Governments, education services and law enforcement) to enhance best practice-sharing.[61] It also foresees a regulator monitoring the implementation of the commitments through a transparent and independent review process.

(b) EU Internet Forum to counter terrorist content online

An EU Internet Forum to counter terrorist content online was established in December 2015 among EU Interior Ministers, high-level representatives of major internet companies (such as Facebook, Google, Microsoft and Twitter), Europol, the EU Counter Terrorism Co-ordinator and the European Parliament[62]. It meets annually and has seen its membership expanded. One of its goals is to reduce accessibility to terrorist content online.

The Forum led to an efficient referral mechanism in particular with the EU Internet Referral Unit of Europol, a shared database of hashes with more than 40,000 hashes of terrorist videos and images. At its third meeting in December 2017, representatives of online intermediaries noted

[59] See https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online.
[60] The firms signatories are: ASKfm, BT Group, Deutsche Telekom, Disney, Facebook, Google, KPN, The LEGO Group, Liberty Global, Microsoft, Orange, Rovio, Samsung Electronics, Sky, Spotify, Sulake, Super RTL, TIM (Telecom Italia), Telefónica, Telenor, Telia Company, Twitter, Vivendi, Vodafone. The associated signatories are: BBFC, Child Helpline International, COFACE, eNACSO, EUN Partnership, FFTelecoms, FOSI, FSM, GSMA, ICT Coalition, NICAM, Toy Industries of Europe, UNICEF..
[61] The common action is complemented by individual company commitments with specific timeline to better protect minors online, see: https://ec.europa.eu/digital-single-market/en/news/individual-company-statements-alliance-better-protect-minors-online.
[62] Commission Press release of 3 December 2015, IP/15/6243.

the increasing use and accuracy of AI, such as photo and video matching and text-based machine learning to identify terrorist content.[63]

(c) Code of conduct on countering illegal hate speech online[64]

A Code of conduct on countering illegal hate speech online was signed in May 2016 by 7 important online intermediaries (Facebook, Microsoft, Twitter, YouTube, Google+, Instagram and Snap Chat) and aims at clear, accessible and effective Notice and take down procedures, removal of the majority of notices within 1 day, and cooperation with trusted flaggers in particular from civil society organisations and awareness campaigns.

The implementation and impact of the Code is assessed every six months by the Commission. The third evaluation of January 2018 shows continuous improvements as 70% of notified illegal hate speech is now removed and more than 81% is removed with 1 day. However, transparency and feedback to users are still unsatisfactory.[65]

(d) Memorandum of Understanding on the sale of counterfeit goods via the Internet

A Memorandum of Understanding on the sale of counterfeit goods via the Internet was signed in 2011 between rights owners, Internet platforms and associations.[66] It aims to improve notice-and-takedown and enhance proactive measures taken by rights owners and online intermediaries, increase cooperation and better fight against repeated infringements. A revised version was signed in May 2016 to include Key Performance Indictors in order to facilitate its monitoring.

The evaluation by the Commission[67] shows that notice-and-takedown measures are useful and have been improved by the MoU but, because they are only ex-post, they need to be complemented by preventive and proactive measures. Those measures require a close cooperation between intermediaries and right holders. They can be supported by automated techniques, although such techniques tend to have many false positives (over-removal) which need to be corrected by human interventions.

---

[63] Commission Press release of 6 December 2017, IP/17/5105. For instance, the Google representative notes that « *98 percent of the videos we remove for violent extremism on YouTube are flagged to us by machine-learning algorithms, up from 75 percent just a few months ago* ».

[64] See http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

[65] Commission Press release of 19 January 2018, IP/18/261.

[66] In October 2017, the signatories were: for the rights owners: Adidas, Chanel, Gant, Lacoste, Luxottica Group, Moncler, Nike and Procter & Gamble; for the Internet platforms: Alibaba, Amazon, eBay, Priceminister Rakuten, Allegro; and for the associations: ACG UK, AIM European Brands Association, Business Action to Stop Counterfeiting and Piracy, Federation of the European Sporting Goods Industry, International Video Federation, Toy Industries of Europe.

[67] SWD(2017) 430.

2.2.4. Conclusion

Although the economic and societal power of some online platforms has increased considerably over time and calls to increase their responsibility are more pressing, the e-commerce Directive, which was negotiated 20 years ago, has not been reviewed. However, the Commission has complemented the Directive by two soft-law instruments, a Communication and a Recommendation, with the aim of providing guidance and principles to the platforms and the national authorities to step up their fight against illegal material online.

These two instruments mainly aim to improve the effectiveness and transparency of the notice-and-takedown process, stimulate proactive measures, and increase cooperation between providers of hosting services and the other stakeholders of the eco-system (in particular users, trusted flaggers and public authorities). Yet, the legal effects of those instruments and their relationship with the e-commerce Directive is not entirely clear. In particular, it is not obvious to us that all the principles of the Communication and the Recommendation directly stem from the Directive and could be made binding via the Directive.

For illegal material that is particularly harmful, the baseline regime of the e-commerce Directive has been complemented over the years by sector rules and co/self-regulation as summarised in Table 1 below. The online diffusion of child sexual abuses is now prohibited by a specific directive and multiple commitments have been taken by digital firms to fight such propagation. Similarly, the online diffusion of terrorism content is prohibited by another specific directive and a multi-stakeholders forum has been set up between the Internet platforms and the enforcement agencies to reduce such diffusion. The online diffusion of hate speech will soon by subject to the revised AVMS Directive and a Code of conduct has been adopted to reduce such propagation. Finally, regarding the online violation of intellectual property rights, a new copyright Directive in the digital single market is being negotiated (with the aim of reducing copyright violation on the Internet) and a Memorandum of Understanding has been concluded between some online platforms and trademark right-holders to reduce the sale of counterfeit products on the Internet.

Table 1: Types of content

Type of illegal content	Hard-law	Soft-law	Co/self-regulation
BASELINE *All types of illegal content online*	- Dir. 2000/31 e-commerce	- Communication 2017 Illegal content online - Rec. 2018/334 Illegal content online	
Child sexual abuse	- Dir. 2011/92 Child sexual abuse		- CEO Coalition (2011) - ICT Coalition for Children Online (2012) - Alliance to Better Protect Minors Online (2017)
Terrorist content	- Dir. 2017/541 Terrorism	- Rec. 2018/334 Illegal content online	- EU Internet Forum
Hate speech	- Dir. AVMS in case of video-sharing platforms		- CoC Illegal hate speech online (2016)
IP violation – copyrighted content	- Prop Dir. Copyright DSM		
IP violation – counterfeit goods			- MoU Counterfeit goods online (2011-2016)

3. Economic analysis of liability rules for online intermediaries

3.1. Preliminaries: economic rationale for liability

3.1.1. Market failures

In this report, we focus on arguments for and against imposing liability on online intermediaries. Before doing so, it is helpful to consider the rationale for liability in general. From an economic perspective, this means assessing which mechanisms are at play that may affect private incentives of the parties involved.

When two private parties voluntarily engage in a bilateral transaction, this should generally be welfare enhancing for both of them. Otherwise they would choose not to conclude the contract. Nevertheless, situations may occur in which a transaction results in harm to an individual, or to society at large. The role of liability rules, from an economic point of view, is therefore to prevent market transactions or activities that result in harm. This prevents harmful bilateral transactions from taking place. Plus, protecting a party in the transaction may actually facilitate beneficial bilateral transactions, as some such transactions may not occur absent liability rules. If markets participants fail to engage in socially beneficial bilateral transactions or conduct transactions to the detriment of society, we speak of market failures. If market failures arise, liability rules or other types of regulatory intervention may be called for in order to prevent or remedy the occurrence of harm.

To determine when and which market failures may arise, it is useful to consider an open market place[68] in which a bilateral transaction between a buyer and a seller may take place. A market failure may arise if i) one of the transacting parties has market power; ii) the parties have asymmetric information regarding the quality of the good or service offered by one party or the monetary or non-monetary transfer to be provided by the counter-party; iii) one or both parties have behavioural biases or limited cognition; or iv) the transaction or activity causes negative externalities on others, meaning that third parties are negatively affected.

3.1.2. Market power

A first possible market failure is caused by market power. If a party, say a firm, has market power, it is not subject to strong competitive pressure from actual or potential competitors. Firms operating in a competitive market cannot afford to raise prices or lower quality without

[68] An open market place is not managed by an intermediary and provides unconstrained access. This serves as a backdrop to our subsequent investigation that includes digital intermediaries.

risking losing most or all customers to competitors.[69] On the contrary, a firm with market power gains control over price and quality and it tends to distort price and quality relative to the social optimum. This is not only detrimental to consumer welfare, but also results in a welfare loss for society. At a higher price, some consumers will no longer purchase the good or service or reduce the transaction volume, even though they value the good or service more highly than what is the opportunity cost to provide the product or service. Hence, mutually beneficial transactions fail to take place, which is reflected by a deadweight loss.

As alluded to above, firms with market power may exploit consumers in ways other than charging high prices. In particular, a firm with monopoly power may choose to offer a quality different from the socially optimal one, since it is concerned about the marginal consumer rather than the average consumer. Thus, the firm may decide against large expenditures in quality improvement, and leave the quality of its product at a socially suboptimal level (Spence, 1975). A low quality stands for high security risks for consumers: either the product is unsafe to use or it has other unwanted side effects.

If the firm does not meet certain quality levels, the government may decide to intervene. It may impose a quality standard through regulation, or it may impose liability to the firm for offering goods or services below a certain quality level. This follows from a theory of a second best according to which regulation of minimum quality is considered, but price regulation is not considered. By intervening, the government effectively decides to restrict the choice for consumers, since goods and services below a certain quality level will no longer be available to them. The higher-quality goods and services that remain on the market may be offered at a higher price, if associated production costs are higher.

An example is food production by a firm with market power: if certain quality standards are not fulfilled, this may pose health hazard to consumers. If the firm has market power, it might have suboptimal private incentives to incur costs to improve its production process and reduce health risks. The reason is that it may not be able to capture all the benefits generated for the quality increases while it bears all the cost. The government can possibly improve the position of consumers and increase overall efficiency, by introducing regulation or imposing liability on the firm if it causes harm to its customers' health. A particularly strong reason for such intervention exists if not all the harm is borne by the consumer, but some of the cost is shifted to third parties, e.g. because treatment costs are covered by the health insurance. Another example is that security risks are not only borne by the buyers, but may spill over to other users.

3.1.3. Asymmetric information

In the previous examples, market power may not be the reason or the only reason why a firm may not take sufficient care to prevent harm caused by its products. Another reason may be

[69] The provision of quality may also be socially inefficient under perfect competition. This is well recognised in the economics literature on innovation incentives. For a textbook treatment see for instance Belleflamme and Peitz (2015).

that the firm is only privately informed about the quality and, thus, knows that its customers lack information to assess the quality of its products. Thus, they have less information about the quality of the product than the seller has, resulting in a situation of asymmetric information.

While this problem is particularly pervasive in the context of market power, asymmetric information problems can arise in competitive markets as well. The classical example of asymmetric information as a market failure is the "market for lemons", as introduced by Akerlof (1970). In his example, buyers in the used-car market value high-quality cars higher than low-quality cars, so-called "lemons". Sellers value cars, high-quality or low-quality, slightly less than buyers do. If buyers can tell high and low quality apart, trade in the market will flourish. However, buyers may not be able to tell whether the car being offered to them is of high or low quality. To account for the risk that the car is of low quality, buyers are willing to pay only a low price. However, sellers who know that they have a high-quality car will reject such an offer. The only sellers who will be prepared to accept the reduced offer will be those who are offering a low-quality car. As a result, high-quality cars will not appear in the markets, and only low-quality ones are traded. The information asymmetry thus leads to (partial) breakdown of the market. However, the problem is not only the initial information asymmetry, but also the fact that sellers of high-quality products cannot credibly convey the quality to buyers. High-quality sellers suffer from the information asymmetry.

Information asymmetries also harm consumers since, in the example, gains from trade with high-quality cars do not materialise. Consumers may actually be harmed when trading if they hold erroneous expectations. This may be the result of informed sellers misleading or cheating consumers. Consumers may be disappointed if they find that sellers have withheld information regarding the quality of their good or service, misrepresented it or even outright lied about the quality of the good or service. The market failure of asymmetric information is a key rationale for consumer protection rules, as consumers may often be at an information disadvantage with respect to the seller. It may also be a main motivation for liability rules. In particular, liability rules may enable firms to credibly disclose information: if wrong claims are sanctioned, a low-quality firm may have little incentive to claim to be of high quality.

However, credible quality assurances can possibly be given by the firm itself (and it may want to do so for dynamic considerations) or by an intermediary, as discussed in Section 4.2. Thus, there may exist private solutions to the possible problem of under provision of quality.

3.1.4. Limited cognition and behavioural biases

In some cases, there is technically no information asymmetry, but the consumer nevertheless does not obtain all the relevant information. Research in behavioural economics has identified a number of heuristics and limited cognition properties that may guide consumer decision-making; these concepts have been applied to market environments (Heidhues and Koszegi, 2018). For instance, if consumers are prone to framing effects and limited attention, sellers may

exploit this by presenting their offers or the specifications in a different way.[70] The sellers still communicate the information, but do so in a way that encourages consumers to ignore negative side effects or quality problems. Consumers may have all the information, but may not properly process it and, thus, may not properly assess the risks or costs associated with the product or service. An example is car rental companies offering complementary insurances to customers at very high premiums, asking customers to opt-out if they do not find it important to be protected against harm.

3.1.5. Externalities

So far, we have considered market failures in which harm affects the contracting parties, but we abstracted from effects on third parties. Situations may also arise in which both contracting parties benefit from the transaction, but fail to take into account that their contract negatively affects third parties. Similarly, one party may unilaterally decide to engage in an activity that negatively affects others.

In both cases, the harmed party is not involved in the decision of the harming parties. In a world without transaction costs, the harmed party may negotiate with the party causing the harm about reducing the harm caused by the activity or transaction. In order to facilitate such negotiations, the law needs to specify the rights of the harmed party vis-à-vis the parties causing the harm (Coase, 1970).

In reality, transaction costs are often too high and negotiation problems too complex to resolve externality problems through private negotiations. For instance, if an activity or transaction harms a large group of people, or even society at large, parties are unlikely to reach a solution. Even if they were able to reach out to each other, the transaction costs of doing so would likely outweigh the benefits to be achieved from reducing the harm. In addition, multi-party bargaining is prone to failure, in particular, if asymmetric information is present. In such cases, negative externalities are a source of market failure. The government may step in and stipulate regulations or impose liabilities with respect to third parties, in order to induce private parties to internalise the harm they may cause to others in their decision-making. In the presence of digital intermediaries, it is also possible that there exist private solutions also to externality problems, as will be discussed in Section 4.2.

3.2. Designing liability rules for online intermediaries

3.2.1. Private interests of online intermediaries

The setting discussed so far concerned bilateral relationship in an open market place. However, many transactions occur on proprietary market places: one where an intermediary manages the

[70] For a simple formal investigation, see Li, Peitz and Zhao (2016).

(online) market place. The environment in which online intermediaries operate is more complex than the traditional market with bilateral exchanges, as was discussed in Section 1.1 above.

In this environment, online intermediaries pursue their private interests. These interests may include collecting profits in the short term and gaining market share or expanding their business for dynamic purposes. In order to achieve these latter goals, online intermediaries may also be interested in maintaining a good reputation with users, advertisers and the public at large. Therefore, when market failures are an issue as part of the bilateral exchanges that online intermediaries facilitate, the intermediaries may have an interest in mitigating the negative results. Arguably, the rise of online intermediaries is closely linked to their success in reducing asymmetric information problems (Belleflamme and Peitz, 2018).

Nevertheless, the self-interest of online intermediaries may not always fully align with societal interests. Typical market failures surrounding bilateral contracts may fail to be prevented, or new market failures may arise in the context of the business activities of online intermediaries. In such cases, public policy may be needed to address these market failures and ensure that private and societal interests are better aligned.

3.2.2. Elements of liability rules

Liability rules are one type of policy intervention that can be employed to better align private and public interests. A liability rule requires a party to compensate any losses its actions cause to others, if this party did not meet a pre-determined duty of care. A first element in designing liability rules is to establish the appropriate duty of care. The duty of care may range between full immunity, in which case there is no liability, and strict liability. If strict liability is imposed, the mere existence of harm and a proximate cause are sufficient to establish tort liability. More common are negligence rules, where the harmed party must demonstrate that the defendant breached a duty of care and, thus, acted negligently.

In demonstrating negligence, the harmed party faces a certain burden of proof. This second element of liability rules affects the parties' costs and risk of enforcing their right.

Thirdly, different types of liability may be imposed. In particular, indirect or secondary liability may play a role next to direct or primary liability. Secondary liability depends on the illegal behaviour of a third party, such as the vicarious liability of employers, or contributory infringements (Sartor 2017:9). Contributory infringement applies where one party knowingly induces, causes, or otherwise materially contributes to the infringing conduct of another (Lichtman and Landes 2003:397). In cases of secondary liability, it is not the wrongful activity itself that triggers liability, but the fact that the party provides the context or enables and facilitates the illegal activity. A rationale for imposing secondary liability is that a party with control over others, and potentially benefiting from their activities, should be encouraged to exercise care in monitoring them. By taking monitoring efforts, these parties can reduce the likelihood of legal infringements and, in turn, reduce harm to others. Another rationale is that

this party may be easier to find and have more financial means than those it oversees, facilitating enforcement by harmed parties (Lichtman and Landes 2003:397-9). In the context of online intermediaries, secondary liability may be relevant as online intermediaries may be able to monitor or regulate their users.

From an economic perspective, the aim of liability rules should be to prevent harm resulting from market failures. Therefore, in order to determine the appropriate liability for online intermediaries, we need to assess which market failures may arise in this context, and under which conditions they are most likely to arise. Specifically, this requires an analysis of when online intermediaries have a private interest in preventing harm from illegal material on their platform. Insofar as intermediaries' private incentives to minimise harm are lower than the public interest in them doing so, a liability rule may benefit society.

3.2.3. Applying the economic theory of tort to online intermediaries

The aim of liability rules to prevent harm resulting from market failures can be specified as follows: the liability rule should aim to minimise the social costs of the risk associated with an activity or transaction, be it through an accident or through intentional harmful behaviour. These social costs of torts are the costs of precaution, the costs of harm and the administrative costs (Calabresi, 1970).

Given that precautionary measures to prevent harm may be costly, a liability rule should not necessarily aim at eliminating harm altogether. A liability rule should induce parties to take precautionary measures insofar as these measures do not cost more than the reduction in expected harm they produce, as stated by the Learned Hand formula.[71] The expected harm consists of the probability that harm occurs, multiplied by the amount of harm in case it occurs. Instead of a single precautionary measure, we could also consider continuous costs of care. For instance, an online intermediary could choose how many resources to spend on monitoring efforts. In such cases, the optimal duty of care should require the marginal costs of precaution to be equal to the marginal benefits they produce, meaning the marginal reduction in expected harm. In the example of monitoring, the marginal version of the Learned Hand formula dictates that online intermediaries should be expected to monitor insofar as an extra euro spent on monitoring results in at least one euro saved in expected costs of harm.

However, the online intermediary may not be the only party that can reduce harm related to the activities of the platform. Other parties, such as users, providers, or third parties suffering harm, may also be able to reduce the risk of harm, or to limit the amount of harm in case the risk of harm materialises. In such cases, we need to establish which party can take precautionary measures at the lowest costs, the so-called "cheapest cost avoider". In many instances, limiting the amount of harm requires the joint effort of some users and the online intermediary. In

[71] The original description of this balancing act by Judge Learned Hand was in United States v. Carroll Towing Co. (1947).

particular, users may inform the online intermediary about harm and the online platform can then take appropriate measures against the party causing the harm. For example, buyers may inform an online trading platform about harmful or illegal products provided by a seller and the online platform can take actions against this seller. These measures include the take-down of sellers and the flagging of certain sellers through a reputation system.

In addition to inducing the optimal level of care, the liability rule ideally optimises the level of a risky activity as well. Decreasing the level of risky activities could limit harm, which is why parties should be encouraged to not only consider how much care to take, but also how often to engage in the risky activity altogether. However, a risky activity may also produce significant social benefits. If a liability rule discourages beneficial activities by making them too costly to engage in, this would be a loss to society. Since online intermediaries affect trade between parties, liability rules regarding the online intermediary indirectly affect the level of the risky activity.

The extent of the harm and costs to prevent it may vary depending on the type of illegal content. As a result, the need for, and design of, a liability rule may differ according to the type of illegal content as well. The economic analysis will address specific issues related to the following types of illegal content where relevant, in line with the typology of the European Commission:[72]

- Incitement to terrorism
- Child sexual abuse
- Illegal hate speech
- Copyright infringement
- Infringement of other intellectual property rights (e.g. counterfeit, design infringements)
- Illegal commercial practice (e.g. scam, fraud, subscription trap)
- Infringement to other community standards or terms of service

In sum, assessing the need for and design of a liability rule requires an overview of i) the precaution costs for the various parties involved (3.2.4), ii) the administrative costs associated with a liability rule (3.2.5), iii) the extent of the harm, and the parties affected by the harm (3.2.6), and iv) the social benefits of the activities that may cause harm (3.2.7). Parties' private costs and benefits of taking precautionary measures, respectively precaution costs and reducing harm to themselves, affect their private incentives to take care. The following subsections assess these private incentives. The goal is to determine whether and to what extent a liability rule may be needed to align private incentives of online intermediaries with the public interest.

[72] DG Connect, Public consultation on measures to further improve the effectiveness of the fight against illegal content online, p. 18, available at https://ec.europa.eu/info/consultations/public-consultation-measures-further-improve-effectiveness-fight-against-illegal-content-online_en.

3.2.4. Precaution costs

Precaution costs in the economic theory of liability are defined more broadly than the costs of preventing that any illegal material shows up on a platform. Precaution costs entail those costs parties make to prevent the harm, reduce the risk of harm occurring, and reduce the amount of harm in case of an accident. Taking precautionary measures often requires money, time, or convenience (Cooter and Ulen, 2016). For users of online platforms, precaution costs may for example arise from exerting effort to obtain more information about a counterparty.

On the side of online intermediaries, precautionary measures may include monitoring and detection efforts and costs to develop detection software, as well as costs of maintaining review systems and notice and takedown systems, including responding to users' notices. Online intermediaries may exert effort to remove or limit access to illegal information or illegal goods or services from a platform. This presumes that the intermediary is aware of the illegal material on its platform, which may not be the case. Precautionary efforts include proactive measures to find the illegal content and to facilitate its reporting, as well as to prevent illegal user behaviour from taking place. Such proactive measures may involve the development of technological tools to detect illegal material more quickly. It also includes measures against violators, such as intermediaries' efforts to filter content in order to prevent illegal behaviour of users, or excluding violators from the platform altogether (Sartor 2017:10).

If precaution costs for intermediaries are high (and associated with low private benefits), intermediaries' incentives to prevent harm may not align with social incentives to prevent harm. Imposing liability on intermediaries may solve this problem by inducing intermediaries to consider not only their precaution costs, but also the costs of harm. However, other parties – suffering the harm, or using the services of the intermediary – may also be able to reduce the risk of harm by incurring precaution costs. In order to determine whether imposing liability on intermediaries is appropriate, we need to determine which party can prevent the harm at the lowest costs. This so-called "cheapest cost avoider" should be liable for the harm.

(a) Injured parties

The possibilities for injured parties to take precautionary measures differ considerably depending on the type of injured party, type of illegal material and type of harm. Buyers and sellers in some cases may be able to reduce the risk of harm by obtaining more information about the counterparty, for instance relying on online intermediaries' user review systems. This is the case in situations where a contracting party may be harmed, such as in cases of fraud or other illegal commercial practices. It may also be true in cases of counterfeit goods and copyright infringements, depending on whether the buyer views these as harm to themselves. The possibilities of buyers and sellers to reduce harm may be reinforced by the intermediary, for instance by enforcing generous return possibilities.

A qualitatively different situation occurs if a contract neither harms the buyer nor the seller but a third party. In such cases, neither contracting party will have an interest in reducing harm (or

reporting it to the intermediary). For instance, parties to a trade in weapons or antiquities are unlikely to engage in costly precautionary measures to reduce the risk of harm associated with this transaction. The party injured by contracts for illegal goods or material is likely a third party who may not have the means to prevent the harm from occurring. One can think of cases in which animals suffer harm, such as illegal trade in exotic animals. Another example would be child pornography. In cases of such serious harm, society at large may have to take precautionary measures to prevent this harm, for instance by increasing criminal sanctions and strengthening enforcement.

In case of intellectual property rights violations, right holders may have the means to reduce the expected harm. They can notify intermediaries about infringements so that the content can be removed. In some cases, right holders may have leverage with intermediaries by threatening to leave the platform if rights violations continue to occur. Right holders may also be able to reduce harm by making it more difficult for violators to use or copy their protected material. For instance, copyright holders may be able to affect the behaviour of users indirectly by protecting access to their works. Technologies are available to encrypt files with the aim to prevent illegal duplication by users. However, this may not work for all types of intellectual property rights violations and all types of buyers. For example, there is little that a trademark holder can do whose sign is used to label counterfeit products (Husovec 2016:12).

Victims of hate speech or discrimination may have little means to prevent the harm, since they likely have no control over the individuals or companies violating their rights. They may not even know the identity of these individuals or companies, or be able to reach them. Their only means to reduce harm may be to notify the online intermediary of the harmful content, so that it can be removed (see further subsection (b) below).

Finally, illegal content can harm society at large but not necessarily an identifiable individual who would be able and willing to notify the content to the intermediary. Particularly in cases of terrorist content, no individual may take action to notify the intermediary, let alone have the means available to reduce the harm of terrorist content in other ways.

(b) Online intermediaries

Particularly in cases where injured parties may not be able to effectively reduce harm, be it with or without the assistance of online intermediaries, a more active role of the intermediary may be appropriate. An online intermediary may have several precautionary measures at its disposal, placing it in a position to limit the illegal behaviour, or mitigate the resulting harm. An intermediary will often be able to exercise influence over the behaviour of its users. It can employ rating systems to improve transparency for users, allowing reputation mechanisms to keep user behaviour in check (Belleflamme and Peitz, 2018). It can also punish misbehaving users by banning them from the platform.

If the intermediary can influence the behaviour of its users or limit the resulting harm, it may still be costly for the intermediary to deploy the measures at its disposal. Several considerations

are relevant to determine the precaution costs of online intermediaries. The costs of detecting illegal material and of removing it may vary depending on i) the size of the platform, ii) the type of harmed party, iii) the intermediary's business model and iv) the type of illegal material.

First, the size of the platform may affect intermediaries' costs of detection, monitoring and removal because of possible economies of scale in precautionary measures. Economies of scale may be more relevant in relation to active monitoring than to passive monitoring. As regards passive monitoring, large intermediaries, with more activity or transactions on their platform, likely deal with more instances of illegal material than small intermediaries do. As a result, they are likely to receive more requests to remove content or offers than small platforms. They may have few means to economise on handling these notifications. However, as regards active monitoring, larger intermediaries may be able to benefit from economies of scale. Because of their large scale, it may pay off for large intermediaries to invest in developing or acquiring software tools to identify and filter out illegal content. Large intermediaries can spread the high fixed costs of such software tools over all instances of illegal material, and cover it with their higher revenues. Also, the precision of warnings generated by software tools may increase with the volume of transactions. Investments in advanced software tools might not pay off for smaller platforms, forcing them to do more detection and monitoring work manually, at higher average costs and less precision per instance of illegal material.

Economies of scale are a relevant consideration in deciding on liability rules for intermediaries, also because of the effects on competition these rules may have. The duty of care imposed by a liability rule results in higher costs of doing business for intermediaries. As a possible downside, this may discourage socially beneficial business activity of intermediaries as it increases the cost of operation; see the discussion in Section 3.2.5. below. If the costs to comply with the duty of care are significantly higher for small intermediaries than for large ones, the liability rule may make doing business too costly for small intermediaries. Large incumbents obtain an advantage as compared to small competitors, potential entrants may be discouraged from entering the market and small intermediaries may exit the market. Thus, there may be a trade-off between static efficiency of liability rules and dynamic considerations that include entry and exit of intermediaries in response to changes of the liability regime. In order to prevent a detrimental effect of liability rules to competition, it may be necessary to determine a threshold for some monitoring obligations. Particularly with respect to active monitoring, where scale economies may be more relevant, small platforms might need to be relieved from some obligations. Static efficiency considerations should prevail if the cost inflicted upon all market participants is considered low, while the expected benefit generated by the liability rule is high. In such cases, it may be preferable to apply a liability rule across the board.

A second determinant of precaution costs may be the type of harmed party. Costs may be lower when harm falls on an individual that has an interest in notifying the intermediary and is in a position to do so. If this is the case, the intermediary may be able to rely largely on responding

to notifications, rather than having to engage in active monitoring; for further discussion see Section 3.2.5. on administrative and enforcement costs.

Thirdly, the business model of the intermediary may affect precaution costs. There are various types of content hosting platforms, ranging from social media providers to e-commerce platforms or document storage services. Some business models may be more prone to being used for illegal purposes than others, or may face more instances of illegal material. In addition, some business models may be more vulnerable to types of harm that are more difficult to recognise than others. For instance, social media platforms may be vulnerable to hate speech or content inciting terrorism, whereas e-commerce or trading platforms may be vulnerable to sales of counterfeit goods or other illegal commercial practices. Regarding intellectual property rights infringements, trading platforms may face relatively low detection costs if trademark holders provide them with notifications to remove the illegal goods from the platform. By contrast, social media platforms may need to spend more resources to address the illegal content if they need employees to review content and determine if it is illegal, rather than relying largely on automated systems.

These examples highlight a fourth determinant of precaution costs: the type of illegal material. Software tools have become available that detect illegal material with increasing accuracy. The performance of these software tools varies considerably depending on the type of illegal material. In some domains, such as copyrighted works, their performance enables an effective and rather precise control (Sartor 2017:22). For some types of content, technologies have been developed to facilitate detection. For instance, Microsoft developed a technology to help identify and remove photos showing child sexual abuse.[73] For other illegal material, content identification technologies may be less effective, or not be economically sustainable.

Automated detection mechanisms may, for instance, function more effectively when a legal infringement is clearly identifiable, than when interpretation is needed to identify the illegality of the material. Some illegal products may not immediately be recognised as illegal, such as counterfeit goods. However, there are markers available that indicate a high likelihood that a product is a counterfeit. Regarding some illegal content, determining illegality may require specific case-by-case review, such as in cases of hate speech or terrorist content. The intermediary may incur higher detection costs if it needs to evaluate each case individually in order to determine whether the material is illegal or infringes on the rights of others. In such cases, technologies for identifying and filtering out illegal content or offers may not function as well as for more easily identifiable material. This means that intermediaries might need to rely more on manual detection by humans in order to detect and remove content, which tends to raise precaution costs. Even if online intermediaries can rely on notifications by users for some types of material, such as fraud on trading platforms, maintaining such a notice and takedown

[73] "Microsoft's PhotoDNA: Protecting children and businesses in the cloud", 15 July 2015, available at https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/.

system is likely to be costly. Therefore, the availability and development of automated tools to detect illegal material may reduce precaution costs of online intermediaries.

Even in areas where detection software is available, it is not always accurate. At the present level of technological sophistication, automated systems cannot fully replace human judgment in detecting illegal material, or flagging the use of material as fair (Frosio 2017:42). When removing material using automated tools, online intermediaries risk on the one hand excluding legal and socially beneficial materials (Type I errors or false positives), and on the other hand failing to exclude illegal materials (Type II errors or false negatives). A high number of Type I errors may reflect over-removal by the online intermediary (Trimble and Mehra 2014). The online intermediary may be tempted to remove too much content, when its costs of doing so are low, and the costs of failing to remove illegal content are high (Urban et al. 2017a and 2017b).

Type I and Type II errors also often occur when human intervention is involved. This may especially be the case when content is removed using a notice and takedown system. Such a system may be less costly for an online intermediary than actively searching for illegal material, since users provide input on the presence of illegal material on the platform. Nevertheless, notices by users may not always be meritorious: they may, instead, reflect the power and means of the requesting party. Particularly in the context of copyrighted material, notice and takedown systems have been linked to Type I errors. Overreaching copyright claims may result in the removal of non-infringing material (Potter 2008:2). When this happens on a large scale, notice and takedown systems may contribute to the erosion of fair use of copyrighted materials. Media companies may use the mass takedown notices instituted through third parties to force online intermediaries to pre-emptively evaluate material that users put online (Doctorow 2008:58). Much of the content that is taken down is the property of independent artists, who then must file reports to get their own copyrighted material back online. The notice and takedown system may produce a chilling effect, discouraging smaller creators to share their work on these online platforms. In such cases, copyright becomes a burden to small content creators, rather than a benefit (Logan 2016:25).

Other negative effects of false positives, such as content incorrectly flagged as copyright protected, are that they undermine freedom of expression and freedom of information (Frosio 2017:42). A fundamental public policy question is to what extent society wants to entrust – and burden – private parties with such a "policing" role.[74] Considering the substantial effects of intermediaries' decisions on notices, some find that online intermediaries weld an inordinate amount of gatekeeping power in notice and takedown regimes (Logan 2016:38-9). Notice and takedown systems resulting in censorship, limitations to free speech and to other fundamental rights may provide an argument against liability of online intermediaries in this context. However, this public policy question of what role private parties and the government should take in combatting illegal material goes beyond the scope of this paper.

[74] See e.g. Belli et al. (2017).

Nevertheless, Type I and Type II errors in removing material should ideally be as low as economically justified. The design of the liability rules may affect the online intermediary's private costs of the occurrence of Type I and Type II errors. The costs of Type II errors or false negatives may be high for intermediaries when liability depends on the knowledge of illegal material of the online intermediary. If the automated content removal system has considered certain material and incorrectly found it to be legal, the online intermediary may be liable, because it had knowledge of illegal material on its platform but failed to take it down. In order to avoid this situation, the online intermediary may be inclined to remove too much, rather than too little material.

Sound legal conditions for liability may prevent over-enforcement by online intermediaries. For instance, clear "Good Samaritan" clause can reassure intermediaries that they will not be held liable for hosting illegal material of which they obtained knowledge through their voluntary, proactive monitoring efforts. Sound legal conditions for liability may also avoid underinvestment by online intermediaries. For instance, in a liability system without a Good Samaritan clause, intermediaries may refrain from voluntary monitoring efforts, because these efforts would lead the intermediary to find more illegal material, which in turn would pose liability risks on them. A Good Samaritan clause removes this "sanction" of voluntary monitoring efforts, which may encourage online intermediaries to take such efforts (Sartor 2017:27). Even if the intermediary may not take down all illegal material it detects through its own active monitoring efforts, this outcome is still preferable to the intermediary not engaging in these active monitoring efforts altogether. It is moreover important for the development of the technologies that online intermediaries are not penalised for their voluntary implementation of content identification technologies (Trimble and Mehra 2014:693).

3.2.5. Administrative and enforcement costs

So far, we have considered costs of intermediaries and other injured parties to reduce the risk or the extent of the harm. We now turn to costs of enforcing a right to compensation based on a liability rule. If parties have few precautionary measures available, they may still be able to enforce their rights against infringers if a liability rule is imposed on the infringers. However, it is costly for users to enforce their rights – potentially more costly than for online intermediaries. In order to determine the cheapest cost avoider, it is necessary to assess how enforcement costs can be minimised.

Victims often face difficulties in obtaining compensation from the primary infringers. It may be impossible or impracticable for victims to identify or sue any of the direct infringers due to the anonymity of the infringer, the cross-border context or merely due to enforcement inefficiency (Husovec 2016:12).

First, the users engaging in the illegal behaviour may be anonymous or not easily reachable (Sartor 2017:10). For instance, compared to an offline shop in a mall, a seller on an online platform may be much more difficult for consumers to track down, in particular in case of cross-

border trade. Similarly, a victim of hate speech on an online platform may not be able to determine the identity of the user expressing the hate speech.

Even if victims do reach the responsible party, they may not be solvent, or the value of the case may not justify engaging in costly proceedings. In that case, the possibility of having recourse to the online intermediary, usually a business with financial resources, would increase the victim's chances of receiving compensation (Sartor 2017:10). Costs of proceedings may be prohibitively high, particularly if victims face a high burden of proof. It may thus not pay off to start proceedings against the party causing the harm at all. This may particularly be the case when harm occurs on a large scale, scattered over a large number of victims or inflicted by a large number of violators. For instance, many people may leave comments containing hate speech to a post someone leaves on a social media platform. In order to enforce their rights, the victim would need to identify, find and sue each one of them.

Enforcement costs are likely to be higher if the defendant is located in another country. In such cases, it is particularly unlikely that the harm justifies enforcement costs for the injured party. Online intermediaries allow for transactions with strangers on a much larger scale, and across much larger geographical distances, than in the offline world. While this clearly creates benefits to society, this also means that victims of harm caused in the context of activity or transactions on online platforms often have few practical means of enforcing their rights against infringers.

Victims may also shy away from court proceedings if they are unsure whether they would be successful in court. Depending on the strength and clarity of the substantial right violated by the infringing party, victims may face uncertainty regarding judges' decisions. Substantial rights may be open to interpretation, or there may be a risk of legal error on the part of the judge.

An important question when extending liability to online intermediaries is whether the online intermediary is complicit in the trade. The intermediary may be considered liable if it did not take measures that are available at reasonable cost to prevent such trade.

3.2.6. Harm

The expected harm that an intermediary creates with its business activity is determined by the gravity of the risk of unlawful user behaviour as well as the seriousness of the damage it may cause. In order to determine whether this expected harm will induce the intermediary to monitor and filter the content or offers on its platforms, we need to examine which parties are likely to suffer the harm. Insofar as the harm falls with third parties, negative externalities are at play. In the context of online intermediaries, users of intermediaries' services may impose negative externalities upon, for instance, the holders of intellectual property rights, such as copyright, design or trademarks (Husovec 2016:7). Harm may also occur between the parties involved in the transaction because of asymmetries of information, or due to cognitive biases on the side of one contracting party.

A self-interested online intermediary would generally be more inclined to incur costs to prevent harm it suffers itself, than harm inflicted on others. But as will be discussed below, harm to others may also translate into economic harm to the intermediaries themselves. Intermediaries may also care about harm to others because of a sense of public obligation or reputational concern.

Nevertheless, absent liability of intermediaries, intermediaries may have suboptimal private incentives to prevent harm caused on others, and exert too little effort to detect and prevent it. In this case, imposing liability on the intermediary may induce the intermediary to terminate or mitigate the consequences of the illegal behaviour of users (Sartor 2017:10).

We recall that several parties besides the intermediary may suffer harm in relation to the business activities of the intermediary: users, providers, intellectual property right holders, or society at large. Depending on who suffers the harm, and what that harm entails, the market allocation may be more or less undesirable for society.

(a) Users

Depending on the type of platform, users may be consumers or sellers of a service or of goods, or they may provide or exchange content (e.g. social media platforms). Users of an online platform may suffer harm in several different ways. First, users may be harmed in the context of their transaction with another user (or seller) on the platform. They may get fewer benefits from the contract than anticipated due to asymmetric information and limited cognition (including outright fraud). Examples of such harm on the buyer side could be non-delivery of products, delivery of faulty goods or of lower-quality goods or services than was promised. Within the context of a contract, users may also suffer damage that exceeds the value of the contract. This may be the case if they receive harmful products or are faced with harmful content. Example are purchasing an app that turns out to be malware and purchasing a good that turns out to be dangerous.

(b) Providers

A specific type of users, providers, may also suffer harm in relation to their activities on online platforms. They may lose the benefits of transactions they engage in with buyers or users in cases of non-payment. Although many intermediaries have mechanisms in place to ensure payment before a good is delivered or service is performed, a provider could face a customer who is unable to pay. In this case, the harm occurs between contracting parties and results from asymmetric information or fraud.

Providers may also suffer damage that exceeds the value of the transaction. An example could be a provider offering a room through an online intermediary, finding out that serious damage was caused to the property after the guests have left.

(c) Third parties

Besides the contracting parties, third parties may be harmed by the activities taking place on online platforms. Harm suffered by third parties reflects the presence of negative externalities.

Users of intermediaries' services may also suffer harm when they were not part of the particular transaction. For instance, users may become the victim of discrimination or hate speech. In the case of discrimination, the user may end up being excluded from a transaction he or she would like to engage in.[75] One could think of a dating website that excludes certain groups of society, or of job recruiters that give preference to certain groups of people when proposing candidates to employers. In the latter case, users may not be aware that they are being discriminated against.

In the case of discrimination and hate speech, the problem is often not one of asymmetric information, but rather of a negative externality. The affected user is a third party to the relationship between the user expressing the hate speech and the online intermediary hosting this content. A user suffers discrimination because information is available to the user engaging in discrimination.[76] Nevertheless, in such cases, the online intermediary may suffer indirect harm as well, as will be discussed further below.

Another group of third parties that may suffer harm consists of intellectual property right holders. If copyrighted material is illegally sold on an online platform by someone else than the right holder, the right holder suffers harm. Similarly, trademark holders suffer harm if counterfeit products are sold online.

Yet, another group may be victims that suffered harm from producing, creating or providing the products, content or services. For instance, individuals who are the victim of certain hate speech. They may be users of the online platform, as discussed above, but they do not need to be. Other examples are child pornography, or exotic animals being traded. In these cases, the parties to the contract may have the perspective that the contract benefits them, rather than harming them. In the former case, the direct victims are the abused children; in the latter, the animals.

In such serious cases, society at large may suffer harm as well. This is also the case for terrorist content, which may, depending on the type of platform, polarise or aid in the preparation of terrorist activities. Society at large may also suffer harm in addition to one of the contracting parties. For example, if a consumer buys an app that turns out to be malware, the consumer might unknowingly spread this around and others may suffer harm as well. Similarly, if a seller sells a malfunctioning scooter online to a buyer, the buyer may end up harming others.

[75] For instance, Edelman et al. (2017) provide evidence for racial discrimination on Airbnb.

[76] However, to the extent that, for instance, racial discrimination is statistical discrimination, more detailed information available to the user can remedy racial discrimination. In this case, the underlying problem is one of a lack of information by the user engaging in discrimination.

It is also possible that both contracting parties benefit from the transaction, but society at large still suffers harm. An example is the trade of antiquities, often to the detriment of cultural heritage. Other examples are parties agreeing on the sale of weapons or of illegal drugs. In the cases mentioned above in which a transaction that causes very serious harm occurs to specific victims, such as the sale of child pornography, society may also suffer harm.

It is noteworthy that cases of harm within the contracting relationship often have spill overs on third parties. Take the case of outright fraud on an online intermediary. Not only does the user suffer harm, the overall effect is that users become less trusting and this may endanger trade between non-fraudulent providers and users; as a consequence, also the online intermediary may suffer from the presence of fraudsters on the platform.

(d) Online intermediaries

In many of the situations described above, the online intermediary involved may also suffer harm. This harm may take several forms, all providing a reason for self-interested intermediaries to monitor trade, guide users and providers, and to remove illegal content or goods from their platforms (Husovec 2016:13).

A first type of harm to the online intermediary may be a reduction in customers or activity on the platform, as a result of deteriorated user experience. Sellers offering illegal content, services or goods may attempt to mislead or defraud users, which may discourage users from using the intermediary's services. The intermediary risks losing users to competitors that offer more trustworthy content or products, or information that is more accurate. In addition to losing participation, the intermediary may also face reduced activity on its platform. Even a monopoly intermediary risks losing some users and a reduced level of activity by others. Troubling content such as pornography and graphic violence may also scare off advertisers, who are not keen on seeing their products paired with an X-rated video or a xenophobic rant (Gillespie 2017:13).

Intermediaries may be particularly interested in preventing harm with respect to injured parties that are important contracting partners for the intermediary. Some right holders might be in a position to leverage their business relationships to induce online intermediaries to take action. For instance, sellers of trademarked goods may learn about trade in counterfeited good on a platform they are active on and complain to the intermediary. They may threaten to leave the platform if the intermediary does not act against the sellers of the counterfeited goods.

A second type of harm for online intermediaries may be to their reputation. In the longer term, the presence of illegal content, goods or services on the intermediary's platform may also harm its credibility and reputation.[77] The intermediary not only risks losing its users, customers or readers, but also advertisers and (legitimate) sellers. Overall, because of reputation and competitive pressure, illegal or fraudulent material may harm the business of the intermediary.

[77] See also Kraakman (1986:56) on reputational concerns and contractual arrangements driving private enforcement.

Because of the threat of losing business or users, online intermediaries may be able to address market failures that persist on open market places. In particular, they may mitigate asymmetric information problems by offering reputation systems. An online intermediary can act on behalf of the prospective buyer to reduce the latter's information disadvantage vis-à-vis the seller. Market power of the online intermediary may limit the incentives of sellers to exploit buyers on the platform. While a seller may be in a strong position vis-a-vis the buyer, it may be weak relative to the platform. Since the intermediary can remove the seller from the platform, the seller may be discouraged from exploiting the buyer. By mitigating asymmetric information problems, online intermediaries may facilitate the functioning of markets that would otherwise break down. For instance, exchanges taking place on Ebay, Uber and Airbnb may not take place if it were not for an online intermediary creating an environment of trust between providers and users.

The incentives of the intermediary to act in this beneficial way may depend on the monetisation instrument it uses. If the intermediary can only charge sellers a fixed payment, and cannot take a percentage of each sale or charge the buyer, it may not have a strong incentive to remedy the asymmetric information problem. The intermediary, in this case, will primarily be interested in collecting fees from the sellers and, thus, focus on seller surplus. When strong (positive) indirect network effects are present, consumer benefits still matter to the intermediary since in that case the number of sellers active on the platform may heavily depend on the number of buyers willing to exchange with them.

An example of an intermediary charging only listing fees are Yellow Pages, which do not monitor or benefit from the transactions on its platform. Currently, many electronic intermediaries do not rely only on listing fees and charge transaction fees as well. Insofar as listing fees form a substantial part of intermediaries' profits, these intermediaries may not have strong incentives to act on behalf of buyers or users on their platforms. Nevertheless, technological developments have allowed intermediaries to better monitor transactions and monetise them. This suggests that extending liability for intermediaries may not be a priority for policy, because intermediaries have strong incentives to prevent harm related to asymmetrical information problems. However, if a group of users suffer from limited cognition and other behavioural biases, intermediaries are less likely to act in the best interest of this group of users.

A third force driving intermediaries to take down illegal content or offers may be the prevention of regulation itself (Husovec 2016:13). Intermediaries may have an interest in combating illegal material on their own initiative, to convince legislators that self-regulation suffices. At the same time, however, the industry might be hesitant to develop tools proactively to detect illegal material, if this may induce legislators to increase their liability. The availability of more advanced or cheaper ways to detect and remove illegal material may provide legislators with an argument to increase the responsibility of online intermediaries.

Alongside these considerations based on profit-maximising incentives, intermediaries may have other reasons to monitor their providers' behaviour and the material on their platforms. Online

intermediaries may be committed to nurturing a healthy community or encouraging creative or innovative offers by their providers. They may also feel a sense of public obligation, especially as a platform grows and exerts greater influence on the public landscape. Finally, they may be sensitive to criticisms levelled by users, journalists, or activists (Gillespie 2017:13), as this affects their attractiveness to employees and investors.

3.2.7. Level of activity

In addition to inducing the optimal level of care, the liability rule ideally also induces the optimal level of activity. Some activities entail a certain risk that harm may occur. The business models of intermediaries, for instance, entail some risks of creating harm. At the same time, however, online intermediaries generate social benefits by providing valuable products, services and content to the wider public. Their self-interest in generating profit also contributes to consumer surplus and promotes innovation.

In theory, a strict liability rule induces the optimal level of activity in addition to inducing the optimal level of care. The reason is that the liable party is encouraged to make a total cost-benefit analysis, including the benefits of the activity, the precaution costs and the expected costs of harm. By contrast, under a negligence rule this party is "off the hook" as long as it takes the required level of care. This encourages the party to take the required level of care, but not to limit the activity level to the socially optimal level.

The drawback of a strict liability rule is that it may also induce parties to limit activities that, while creating a risk of harm, are overall beneficial to society. Intermediaries generally create social benefits through their business activities. This may not be the case for all intermediaries, as a small fraction may focus primarily on socially harmful activities. One could think of intermediaries dealing with illegal exchanges in the "dark web", or intermediaries focused solely on allowing the illegal exchange of copyrighted materials or counterfeited goods. Nevertheless, for the most part, intermediaries enable socially beneficial activities.

Ideally, the liability system does not discourage these socially beneficial activities. At the same time, it should provide sufficient deterrent effect to intermediaries that enable the type of harmful activities described above. A duty of care for intermediaries with respect to illegal material may raise market entry costs, discouraging the beneficial activity of these intermediaries.

The goal of promoting intermediaries' socially beneficial activities therefore forms a first rationale for exempting intermediaries from liability for illegal material on their platform. To the extent that liability would induce intermediaries to abandon or limit their services, liability would negatively affect not only the intermediaries, but also the users of the intermediaries' services (Sartor 2017:11).

A related rationale is to preserve the particular business models of some intermediaries. Business models in which services or content are provided for free may not be sustainable when

intermediaries are subjected to liability, since revenues may not cover the expected damages payments (Sartor 2017:11). Whereas for-profit intermediaries may collect sufficient revenues from advertisers to cover liability costs, non-profit platforms such as Wikipedia may not be able to do so.

Arguably, these two rationales were stronger at the time the e-commerce Directive was adopted than they are now, since several of today's platforms are large and profitable ventures. These intermediaries can be expected to have sufficient resources to cover liability. Nevertheless, small players and non-profit entities are still active in the market, and, from a competition perspective, it may be desirable to ensure their financial sustainability (Sartor 2017:11).

A third reason against intermediary liability is still of high relevance today: liability may induce intermediaries to impede even lawful, and socially valuable activities of their users, in order to avoid the risk of facing liability (Sartor 2017:11). Many online intermediaries host and organise user content. These include Google Search and Bing, as well as user-upload services such as Facebook, YouTube, Twitter, Tumblr, Pinterest, Google+, Instagram, Snapchat, Apple App Store and Google Play, Medium and Blogger, Foursquare and Nextdoor, Tinder and Grindr, Etsy and Kickstarter, Whisper and Yik Yak. Online intermediaries generally do not produce the content, but they make important choices about that content: what they will distribute or prioritise and to whom; how they will connect users and broker their interactions; and which content they will refuse (Gillespie 2017:1). Liability for illegal content would, in many cases, require online intermediaries to make judgment calls regarding the content they host. This, in turn, raises concerns regarding censorship. It also raises concerns about inhibiting entry by providers of products and services.

3.3 Interim conclusions

To summarise, from an economic perspective, liability rules should aim at minimising costs of harm that result from activities or transactions; market failures may lead to such harm.

In the context of online intermediaries, the well-known sources of market failure may come into play: asymmetries of information, market power, and negative externalities may be present in isolation or in combination. Online intermediaries may want to and be able to mitigate some market failures. In particular, online intermediaries may reduce asymmetric information problems and allow markets to function that could not be sustained in the pre-Internet era. In case of negative externalities, third parties are affected by a transaction or activity on an online platform, as may be the case with illegal content. Online intermediaries may also take measures against negative externalities, insofar as they suffer economic or reputational harm, or when they have a sense of public obligation to intervene.

Determining the efficient level of care for online intermediaries involves a difficult balancing act. First, the policy maker has to consider the **instruments available to online intermediaries to**

prevent harm, and the social costs of these precautionary measures. These costs should be compared to the costs of instruments available to injured parties, in order to determine which party can reduce the costs of harm most effectively. Generally, when monitoring costs for online intermediaries are low, they may be best placed to remove illegal content and prevent harm. In cases where online intermediaries are best placed to monitor and control the behaviour of users, and subsequently reduce the expected harm, some form of liability for the intermediary may be appropriate. In such cases, intermediaries may well be interested in monitoring on their own initiative as well. If this were the case, the duty of care would not significantly change their monitoring efforts and the policy intervention may be almost neutral. Insofar as online intermediaries do not engage in cost-effective monitoring on their own initiative, liability rules are likely to induce these intermediaries to take some measures to reduce the costs of harm.

While encouraging online intermediaries to monitor and remove illegal material, ideally the legal requirements for liability also induce online intermediaries to do this diligently. On the one hand, online intermediaries could be encouraged to take proactive, voluntary measures to monitor and remove illegal material. To foster these incentives, an online intermediary should not be sanctioned in cases where it has learned about illegal material through its own voluntary efforts, but failed to take it down (Type II error: under-removal). Put differently, liability rules should not put a sanction on a Type II error by a proactive online intermediary. This may warrant a clear Good Samaritan clause, as will be discussed in Section 4.

On the other hand, the liability rule should discourage online intermediaries from taking down too much content or offers, including legal material (Type I error). If online intermediaries are only sanctioned for failing to remove illegal material, but not for systematically removing legal material in the process, they may be induced to remove too much material. This may be problematic, because it may limit freedom of speech and efficient business transactions. For instance, small artists may not be able to distribute their work if online intermediaries remove it in response to aggressive notifications by alleged copyright holders. A sanction on systematic Type I errors in monitoring may need to be introduced in order to encourage online intermediaries to improve the quality of their notice-and-takedown systems and further develop detection technology.

Secondly, the **type and extent of the harm as well as the type of harmed party** may influence the need for liability of online intermediaries. Generally, the more serious and the larger the harm, the more reason there is to take regulatory action to prevent it. Additionally, the more dispersed the harm, the less likely it is that victims are able to prevent harm themselves or enforce their rights (in particular, in jurisdictions in which class action suits are not possible or face hurdles). In cases where harm is serious and dispersed, there is a stronger argument for some form of liability for online intermediaries. Different types of online intermediaries may be vulnerable to different types of harm, depending on the type of content hosted on their platforms, and more generally on their business model.

Thirdly, the policy maker has to balance the costs of monitoring and the extent of the harm with the **social benefits that the activities of online intermediaries provide to society**. Liability for harm caused by the activities of online intermediaries increases the costs of doing business, and may prevent some business models from being commercially exploited at all. Moreover, small online intermediaries or new entrants may be disproportionally affected by liability rules, which leads to a regulatory barrier to entry. They may not be able to develop or acquire technologies to reduce the costs of monitoring, and, therefore, not achieve economies of scale in monitoring in the way that large incumbents can. For this reason, imposing a high duty of care on all online intermediaries may tip the scale in favour of large incumbents and affect the viability of competition in the market.

Overall, from an economic perspective, there is likely no one-size-fits-all liability rule for all types of intermediaries and all types of harm. Ideally, the **duty of care for online intermediaries varies depending on a range of different factors**, including the level of precaution costs of the intermediary, the possibility for victims to notify or even prevent harm, and the extent of the harm. While practically it may not be possible nor desirable to impose liability exactly along the lines of economic determinants, these factors for differentiation may inform policy makers as to the appropriate type of duty of care for online intermediaries.

As Table 2 indicates, the type of harmed party, their possibilities to prevent harm and the available instruments to the online intermediary may vary depending on the type of illegal material. Material that infringes intellectual property rights harms the right holder, and harms the buyer if they did not intend to buy illegal material. In this case, both asymmetric information and negative externalities play a role.

If the buyer intended to buy illegal material, as may be the case with counterfeit goods and illegally copied copyrighted content, the buyer will not identify as a victim and likely not notify the platform. In this case, a pure negative externality problem is present. This is also likely to be the case for terrorist content and content showing child sexual abuse. Victims of such illegal material will generally not be part of the transaction and may have limited means to prevent harm. In cases of intellectual property rights infringements, injured parties may be large companies with means to enforce their rights and the ability to exert pressure on the platform. However, victims of terrorist content and child sexual abuse content are much less likely to be in a position to notify the online intermediary or exert pressure to remove the content. Similarly, in cases of illegal hate speech, victims may be individuals with limited means to enforce their rights and may need to rely on the automated detection tools or notice and takedown systems of online intermediaries.

In these cases, reputation and a sense of public obligation may induce most well-respected online intermediaries to exert considerable monitoring effort. For such intermediaries, any factor that affects their reputation may also raise a risk of losing customers, given that these customers may generally be less likely to engage if the community on the platform is saturated with hate speech, for instance. Nevertheless, the seriousness of the harm may require a tougher

liability standard for such types of content to induce *all* online intermediaries to monitor and remove such content.

Overall, in cases where the harm is serious and the possibilities for injured parties to notify or otherwise enforce their rights are limited, additional responsibilities for online intermediaries may be appropriate. The next section discusses how this could be achieved through different hard law and soft law instruments.

Table 2: Harm differentiated for types of illegal material

Harmed party →	Contracting party / user (Information asymmetry)		Third party (Negative externality)		Online intermediary		Implications duty of care		
Type of content ↓	Harmed party	Available Measures	Harmed party	Available Measures	Type of harm	Available Measures	Extent of the harm	Dispersion of harm	Need for duty of care online intermediary
Incitement to terrorism	-	-	Victims; Society	Limited	Reputation	Remove content	Very high	High	Strong
Child sexual abuse	-	-	Victims; Society	Limited	Reputation	Remove content	Very high	High	Strong
Illegal hate speech	User	Notification	Victims; Society	Notify online intermediary	Reputation	Remove content	High	High	Strong
Copyright infringement	Possibly buyer/user	Notification, if identifies as victim	Right holder	Notify online intermediary	Fewer customers/ less activity	Remove content; Block seller	Moderate/High (Monetary)	Low	Moderate (if effective notice-and-takedown system)
Infringement of other intellectual property rights (e.g. counterfeit, design infringements)	Possibly buyer/user	Notification, if identifies as victim	Right holder	Notify online intermediary	Fewer customers/ less activity	Remove content; Block seller	Moderate/High (Monetary)	Low	Moderate (if effective notice-and-takedown system)
Illegal commercial practice (e.g. scam, fraud, subscription trap)	Buyer/seller /user	Notification, consumer law instruments	-	-	Fewer customers/ less activity	Remove content; Block seller	Moderate/High (Monetary)	Varies	Moderate (if effective consumer protection mechanisms)
Infringement to other community standards or terms of service (e.g. dangerous products (malware, arms), discrimination, trade in exotic animals)	Buyer/seller/ user	Notification, if identifies as victim Public enforcement tools	Victims; Society	Depends	Reputation Fewer customers/ less activity	Remove content, notify public authority	Varies	High	Moderate to strong (need for cooperation with government authorities)

4. Policy Recommendations

In this last Chapter, we provide recommendations how to improve the legal regime on the liability of providers of hosting services, based on the learnings of the economic analysis of law. First, we recall that tackling illegal material online is a problem of many hands and many rules. These rules need to be consistent internally and effective in giving the many hands the right incentives to police the Internet. Second, regarding the liability rules of the providers of hosting services, we recommend to maintain the liability exemption of the e-commerce Directive but to link it with the provision of an infrastructure allowing effective detection and removal of illegal material. Finally, regarding the liability rules of the 'other hands' (the victims, the providers of material and the authorities), the rules should also give them incentives to contribute to the detection and the removal of illegal material.

4.1 Tackling illegal material online is a shared responsibility

In our view, the regulatory framework to tackle illegal material on the Internet should be guided by three criteria.

1. First, the presence of illegal material on the Internet involves many actors (providers of material, platforms, victims, public authorities, etc.), which are regulated by several rules. Those rules include the liability regime, but also consumer protection, data protection, product safety, and antitrust rules. Thus, **liability rules of the online intermediaries are only one piece, important but not unique, of a broader regulatory framework. We should aim to ensure that all those rules, liability and otherwise, are consistent with each other** at the national level and between the EU and the national levels. Moreover, we should aim for these rules to **give incentives for an effective detection and removal of illegal material**.

Consumer protection rules and, when personal data are involved, personal data protection rules, should reduce information asymmetry and ensure transparency of the liability standard of the intermediaries and the providers as well as, to the extent possible, of the decisions made by automated tools and algorithms. Antitrust rules should contribute to effective competition between online intermediaries which in turn can, under many circumstances, give them incentives to tackle illegal material as a way to differentiate their services on quality.[78]

2. Secondly, the **liability rules in this overall framework should efficiently share the responsibility for the detection and the removal of illegal material online among the many actors involved** in the diffusion of such material. Helberger et al. (2018) appropriately suggest moving from a system of contested liability to a system of cooperative

[78] It is beyond the scope of this report to go beyond these general statements regarding consumer protection, personal data protection, and competition rules.

responsibility. Thus, the liability regime of the online intermediaries is only one part of a broader liability framework which should be consistent and efficient in tackling illegal content/products.

This is also why two extreme solutions should typically be avoided when determining the liability of online intermediaries: a full liability exemption and strict liability. A full liability exemption is problematic, because intermediaries should be induced to cooperate to the detection and the removal of illegal activities on the Internet. Shielding online intermediaries from all liability if they do not cooperate would not contribute to this goal. A strict liability rule, by contrast, shifts too much of the burden of 'policing the Internet' on online intermediaries.

3. Thirdly, **liability rules of providers of hosting services should be principles-based** to be easily adaptable to technology and business models, which evolve quickly and often in unpredictable ways. These principles-based rules could be **clarified by the European Commission in delegated or implementing acts or interpretative guidance**, which can easily be adapted to technology and market evolutions. In particular, guidance prevents that the liability rules remain vague, and ensures that online intermediaries have the necessary knowledge and legal certainty to fulfil their obligations and responsibilities.

Liability rules may also be **complemented with co-regulation or self-regulation** such as codes of conduct. These codes should be drafted in collaboration **with all stakeholders**. Involvement of different types of stakeholders is important to ensure that the diversity of interests is represented and the codes are sufficiently balanced. The implementation of these codes should **be closely monitored** and in case of weak enforcement, remedial actions should be adopted either by the stakeholders or by the State.

4.2 Liability of providers of hosting services

4.2.1 A radical reform: harmonising the liability rules of providers of hosting services

On the basis of the economic analysis of liability rules, **the preferred approach would be a negligence-based system. The duty of care of the providers of hosting services should be determined on the basis of general criteria such as the instruments available to prevent harm and the social costs of these precautionary measures, the type and the extent of the harm and the type of the harmed party, and the social benefits that the activities of online intermediaries provide to the society**. Based on these criteria, the required level of care would ideally be differentiated according to the type of illegal material.

These criteria for the duty of care could be specified at the EU level because of the important cross-border dimension of many e-commerce services. In the specific case of secondary liability of online intermediaries for copyright violations, Nordemann (2018:25) recommends the

introduction of liability rules at the EU level in order to create a level playing field in the digital single market.[79] Nevertheless, such harmonisation would have to be considered carefully, with its benefits but also possible costs in mind. For instance, the impact on the internal coherence and consistency of the civil laws of the Member States would have to be considered when creating specific liability rules at the EU level for specific types of claims.[80]

However, we recognise that due to political economy considerations, **an EU harmonisation of the national rules for secondary liability of online intermediaries is probably not reachable at this stage** for several reasons. It is much more difficult politically and legally to harmonise national liability rules, which are among the most fundamental pieces of any legal system, than to harmonise the exemptions to such liability. Moreover, any tentative to radically change the current system which is not fundamentally flawed[81] risks creating more harm than good, in particular for some types of illegal material where political lobbying is extremely intense. Finally, as noted by Litchman and Landes (2003) in the US context, designing the exemption to liability may lead in practice to very similar results as designing the liability itself. In fact, the majority of the literature does not call for fundamental overruling of the e-commerce Directive but only for adaptations.[82]

4.2.2 A modest proposal: linking the liability exemption to the provision of an infrastructure facilitating detection and removal of illegal material

Therefore, we recommend a solution consisting of maintaining the current exemption system with improvements to ensure, following of Helberger et al. (2018:3), that: '*platforms have an obligation to create the* conditions *that allow individual users to comply with their responsibilities*'. Therefore, we suggest to clarify at the EU level the conditions under which the providers of hosting services benefit from the liability exemption and to link these conditions to the provision of an infrastructure allowing effective detection and removal of illegal material. Such infrastructure should be practicable and proportionate taking into account the characteristics of hosting providers. Many features of this infrastructure are already mentioned in the Commission Communication of September 2017 on tackling Illegal content online and in the Commission Recommendation of March 2018 on measures to effectively tackle illegal content online.[83]

[79] Sartor (2017:28) also mentions the importance of EU harmonisation with regard to the liability regime of online platforms.
[80] Next to, for instance, the rules for antitrust damages actions and laid down in Directive 2014/104/EU, O.J. 2014 L 349/1.
[81] In its Communication on online platforms COM(2016) 288, p. 8, the Commission notes that the public consultation showed a broad support for the existing principles of the e-commerce Directive.
[82] Husovec (2017); Montero (2011); Nordemann (2018); Sartor (2017); Van Eecke (2011).
[83] Some characteristics are also mentioned in the new Article 28a of the revised AMVS Directive. However, our proposal is more modest than the AVMS Directive because we propose to condition the liability exemption to the

1. Improving the detection of illegal material

Illegal material can be detected by online platforms themselves with proactive monitoring measures or by users of the platforms notifying the illegality. EU rules should incentivise platforms and users to detect illegality while minimising the risks and the costs of errors and ensuring a fair balance between the different human rights at stake. While achieving such optimal rules may be challenging in practice, several concrete improvements may contribute to better detection of illegal material.

Regarding the **detection by providers of hosting services**, **proactive measures should be encouraged when they are appropriate, proportionate and specific** in order to reduce the risks of type II errors (under-removal).[84] This implies that the possible current dis-incentive to use proactive measure brought by Article 14 of the e-commerce Directive should be removed and a Good Samaritan clause should be affirmed explicitly to ensure that the providers of hosting services taking on proactive measures are not treated in a less favourable way than the ones not taking these measures.[85] Such a Good Samaritan clause should aid platforms when taking voluntary measures, by removing the risk of being sanctioned for under-removal. This encouragement of specific and proportionate measures should not lead to a general monitoring undermining several fundamental rights.

Regarding the **detection by users**, **the notice-and-take down system should be facilitated and based on common principles defined at the EU level** (also Sartor, 2017; Husovec, 2017). This has several consequences. First, providers of hosting services should set up mechanisms for notices that are easy to access, user-friendly and allow for automated submission.[86] Secondly, they should clearly communicate this possibility to their users.

The progress in artificial intelligence allows platforms and some large users to rely increasingly on automated tools to detect illegal activities on the Internet. Thus, **reliance on automated detecting tools by intermediaries or users should be encouraged as an effective detection means, provided some safeguards are in place**. Given the early developments of these technologies and their rapid improvement over time, it is probably too early to regulate the use of these automated tools. Moreover, this is part of the wider debate on the EU regulation of Artificial Intelligence.[87] However, stakeholders and authorities should **reflect upon at least three types of safeguards**. (i) first, the **minimisation of errors** and the complementary action of humans when the risks and the costs of errors are considered to be too high; (ii) second, the **understandability of the process** and the possibility to give an explanation when content or a

provision of measures for effective detection and removal of illegal content but we do not propose to impose those measures.

[84] To take the formulation of para 18 of the Commission Recommendation 2018/334.

[85] Also in this sense, Sartor (2017:29) As already explained, the Commission considers that the Good Samaritan clause is already compatible with the e-commerce Directive: Communication on tacking illegal content online, COM(2017), p.13.

[86] Commission Recommendation 2018/334 on tacking illegal content online, para 5.

[87] See Communication from the Commission of 25 April 2018, Artificial Intelligence for Europe, COM(2018) 237

product is removed after an automated detection; (iii) third, the need to **share these technologies** between large intermediaries, which have the data, the expertise and the financial means to develop automated techniques, and the small or new intermediaries.[88]

2. Improving the removal of illegal material

Once illegal content or product has been detected, the providers of hosting services **should act expeditiously**, especially when the harm can be important and quickly inflicted and/or when the illegality is notified by an enforcement authority or a trusted flagger.[89]

To reduce the risks of type I error (over-removal) and ensure an appropriate balance between human rights, the platform should, when practical and proportionate, first **inform the provider** of the intention to remove the supposedly illegal material and the reason of such removal as well as give them the possibility to contest such removal by submitting a **counter-notice**. Then, the platform should only remove the material after having assessed in a diligent manner, on the basis of the information given, the validity and the relevance of this counter-notice. However, in exceptional circumstances, when the illegality is manifest and relates to serious criminal offences involving a threat to the life or safety of persons, content may be removed immediately. Also, the platforms should not divulge information which may undermine public policy and public security.[90]

Moreover, online platforms should be encouraged to contribute to the establishment of **out-of-court dispute resolution mechanisms** allowing the material provider whose counter-notice was not followed to contest the removal with a mechanism which is easily accessible, effective, transparent and impartial and ensuring that the settlements are fair and in compliance with the applicable law.[91]

3. The differentiation of care

The economic analysis in Section 3 has shown that **the efficient level of care for the provider of hosting services may vary depending of the level of harm or the dispersion of the victims**. Therefore, for material when the harm is particularly high and/or the victims are particularly dispersed, the level of care of the platforms should be higher.

For instance, for terrorism content, the Commission Recommendation of March 2018 already provides for a stricter duty of care. Similarly, the revised Audiovisual Media Service Directive provides for a different duty of care according to the nature of the content, the harm it may cause, the characteristics of the category of persons to be protected and the rights and legitimate interests at stake.

[88] Commission Recommendation 2018/334 on tacking illegal content online, para 28. This is the case Microsoft' Photo DNA fighting the diffusion of child abuse material: https://news.microsoft.com/en-gb/2013/11/18/tacklingproliferatio/.
[89] *Ibidem*, para 23 and 25.
[90] *Ibidem*, para 9-13.
[91] *Ibidem*, para 14. Also Report of the Special Rapporteur of the United Nation of 6 April 2018 on the promotion and protection of the right to freedom of opinion and expression.

For types of harm that affects users or consumers who have an interest in preventing or mitigating this harm, the policy focus could also be more on empowering these harmed parties to enforce their rights through, for instance, consumer protection mechanisms. Finally, in cases where the harm affects larger parties with sufficient means to enforce their rights, such as is often the case for intellectual property rights infringements, policy makers ought to keep in mind that notice-and-takedown systems work in a transparent and balanced way.

We suggest complementing those reforms related to the baseline liability regime applicable to all types of illegal material **with effective co/self-regulation instruments for specific types of material where additional care is required**. Thus, for the types of material which justify a particularly high duty of care, industry, users and authorities should agree on Codes of conduct specifying in more detail the actions, the timing and the cooperation to ensure rapid detection and removal of particularly harmful content.

4.3 Responsibility of other actors and the public authorities

Next to the providers of hosting services, the other private actors involved in the value chain and the judicial and administrative authorities should also contribute to a safe Internet and to the effective detection and removal of illegal material online. Here also, we follow Helberger (2018:11) for whom cooperative responsibility, '*involves all stakeholders and can take different forms for each: a) organizational and design responsibility for platforms, b) active participation, empowerment, and real responsibility for users, and c) creating frameworks for shared responsibility and shared values for governments, considering platforms and users as partners in regulation rather than as subjects*'.

Victims of illegal content

The victims of the illegal material, or their legal agents or representatives, should notify to the hosting platforms violations when they are the best placed to do so and communicate all the necessary information for the platforms to decide about the removal. They should also be condemned in case of manifestly abusive notices.[92]

Content providers

Unless there are exceptional circumstances, the providers of material should be informed by the platforms of the removal and have the possibility to contest such removal with a counter-notice, then an out-of-Court dispute resolution mechanisms and, ultimately, before the judicial Courts. The inaction of the content providers in case of over-removal may, under some circumstances, lead to losing any right of compensation.

[92] *Ibidem*, para 21.

Administrative and judicial authorities

Finally, national enforcement authorities and online platforms should closely cooperate in ensuring the detection and the removal of illegal material, especially for content that authorities are best placed to identify.[93]

Moreover, the national enforcement authorities should closely cooperate with each other at the EU level and with the European Commission, given the often cross-border nature of the presence of illegal material and its harm.

4.4. Conclusion

Online hosting platforms have gained increasing economic and societal importance in the last decade. This report considered if and how this growing importance ought to affect their liability when hosting illegal material.

When we abstract from the regulatory reality, an economic analysis of liability rules for online platforms points towards a negligence-based system as the preferred approach. Depending on the extent and dispersion of the harm, as well as the monitoring costs of all parties involved, the required level of care would ideally be differentiated according to the type of illegal material.

However, in reality, an elaborate system of rules already exists regarding the responsibility of online platforms. Whereas the e-commerce Directive includes an exemption for online intermediaries, this in practice does not give online intermediaries a 'free pass' to host illegal content.

Nevertheless, the current regulatory framework regarding the responsibility of online platforms can be improved in several concrete ways. Primarily, the law should encourage all parties involved to contribute to tackling illegal material, making this a shared responsibility. This means that it should be clarified at the EU level under which conditions hosting platforms may benefit from the liability exemption. In particular, these conditions should focus on online platforms providing an effective infrastructure allowing efficient detection and removal of illegal material.

Other concrete improvements could help ensure that online intermediaries are encouraged to remove illegal material, and to do so in a diligent manner. Specifically, a Good Samaritan clause should be affirmed, and transparent procedures for counter-notice should be ensured in online intermediaries' notice-and-takedown systems. Overall, EU rules should incentivise intermediaries and users to detect illegality, while minimising the risks and the costs of errors and safeguarding a balance between the different human rights at stake.

On a more general level, we have identified several considerations to guide policy makers in further improving the regulatory framework regarding online intermediary liability. First, the regulatory framework should be made of different rules aiming for consistency with each other

[93] *Ibidem*, para 22-24.

at the national level and between the EU and the national levels. Liability rules are one aspect of a broader regulatory framework to ensure well-functioning markets, including also consumer protection, data protection and competition rules. Second, the liability rules of online intermediaries should be principles-based to be easily adaptable to technology and business models, which evolve quickly and often in unpredictable ways. Third, the liability rules may also be complemented with co-regulation or self-regulation such as codes of conduct. Finally, the liability rules in this overall framework should ensure that the detection and the removal of illegal content or products is a shared responsibility among all the actors involved in the presence and prominence of these illegal materials.

References

Akerlof, G.A. (1970), “The Market for "Lemons": Quality Uncertainty and the Market Mechanism”, The Quarterly Journal of Economics 84(3), pp. 488-500.

Belleflamme, P. and M. Peitz (2015), *Industrial Organization: Markets and Strategies*, 2nd edition, Cambridge University Press.

Belleflamme, P. and M. Peitz (2018), “Inside the Engine Room of Digital Platforms: Reviews, Ratings, and Recommendations”, in: J. J. Ganuza and G. Llobet (eds.), *Economic Analysis of the Digital Revolution*, Funcas Social and Economic Studies nº 4, Funcas.

Belli, L., P.A. Fransisco and N. Zingales (2017), “Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police”, in: L. Belli and N. Zingales (eds.), Platform Regulation. How platforms are regulated and how they regulate us, FGV Direito Rio, pp. 41-64.

Calabresi, G. (1970), *The Costs of Accidents,* Yale University Press.

Calabresi, G. and D.A. Melamed (1972), “Property Rules, Liability Rules, and Inalienability: One View of the Cathedral”, Harvard Law Review, pp.1089-1128.

Cooter, R. and A. Porat (2014), *Getting Incentives Right: Improving Torts, Contracts and Restitution,* Princeton University Press.

Cooter, R. and Ulen, Th. (2016), *Law and Economics, 6th edition*. Berkeley Law Books.

Coase, R. H. (1937). "The nature of the firm", Economica, 4(16), pp. 386-405.

Copenhagen Economics (2007), *Economic impact of the electronic commerce Directive*, Study for the European Commission.

Copenhagen Economics (2015), *Online intermediaries: Impact on the EU economy*, Study for EDIMA.

Doctorow, C. (2008), *Content: Selected Essays on Technology, Creativity, Copyright, and the Future of the Future*, San Francisco: Tachyon Publications.

Edelman, B., M. Luca, and D. Svirsky (2017), “Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment”, American Economic Journal: Applied Economics 9, pp. 1-22.

Floridi, L. and M. Taddeo (2017). *The responsibility of Online Service Providers,* Springer.

Frosio, G. (2017), “Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy”, Northwestern University Law Review 112, pp. 19-46.

Gasser, U. and W. Schulz (2015), *Governance of Online Intermediaries Observations From a Series of National Case Studies*, Berkman Center Research Publication 2015-5.

Gillespie, T. (2017), “Governance of and by platforms”, in: J. Burgess, Th. Poell, A. Marwick (eds.), *SAGE Handbook of Social Media*.

Hamdani, A. (2002), “Who’s Liable for Cyberwrongs”, Cornell Law Review, 87(4) pp. 901-957.

Helberger, N., J. Pierson and T. Poell (2018), “Governing online platforms: From contested to cooperative responsibility”, The Information Society 34(1), pp. 1-14.

Heidhues, P. and B. Köszegi (2018), “Behavioral Industrial Organization”, forthcoming in B. Bernheim, S. Dellavigna, D. Laibson (eds.), *Handbook of Behavioral Economics*, Elsevier.

Hylton, K.N. (1996), “Missing Markets Theory of Tort Law”, Northwestern University Law Review 90, p. 977.

Husovec, M. (2017), *Injunctions Against Intermediaries in the European Union: Accountable But Not Liable?*, Cambridge University Press.

Keats Citron D. and B. Wittes (2017), “The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity”, University of Maryland - Legal Studies Research Paper 2017-22.

Kim, J.Y. (2006), “Strict liability versus negligence when the injurer's activity involves positive externalities”, European Journal of Law and Economics, 22(1), pp.95-104.

Kohl, U. (2012), “The rise and rise of online intermediaries in the governance of the Internet and beyond – connectivity intermediaries”, International Review of Law, Computers and Technology 26(2-3), pp. 185-210.

Kraakman, R.H. (1986), “Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy”, Journal of Law, Economics & Organization 2(1), pp.53-104.

Landes, W. and R.A. Posner (1987), *The Economic Structure of Tort Law,* Harvard University Press.

Landes, W.L. and D. Lichtman (2003), “Indirect Liability for Copyright Infringement: An Economic Perspective”, Harvard Journal of Law and Technology, 16, p. 395.

Léonard, T. (2012), “L’exonération de responsabilité des intermédiaires en ligne: un état de la question“, Journal des Tribunaux, pp. 815-816.

Li, S., M. Peitz, and X. Zhao (2016), “Information disclosure and consumer awareness”, Journal of Economic Behavior & Organization 128, pp. 209-230.

Logan, L. (2016), “Free Expression, Privacy, and Intellectual Property Online: Contesting Intermediary Liability”, Communication Law Review 16(1), pp. 24-42.

Martens, B. (2016), “An Economic Policy Perspective on Online Platforms”, JRC Technical Report, Digital Economy Working Paper 2016/05.

Montero, E. (2011), “Le régime juridique des sites de vente aux enchères sur Internet“, Droit de la consommation-Consumer Recht 90, pp. 56-102.

Nordermann, J.B. (2018), *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, In-Depth Analysis for the IMCO Committee of the European Parliament.

OECD (2010). *The Economic and Social Role of Internet intermediaries.*

Posner, R. (2003), *Economic analysis of law,* Aspen Publishers.

Potter, Trevor. Trevor Potter to Chad Hurley, Zahavah Levine, and William Patry, October 13. 2008; https://www.eff.org/files/mccain_youtube_copyright_letter_10.13.08.pdf.

Sartor, G. (2017), *Providers Liability: From the eCommerce Directive to the future*, Study for the European Parliament.

Schäfer, H.-B. (2001), ‘Tort Law: General’, B. Bouckaert, G. De Geest (eds.), *Encyclopedia of Law and Economics: Volume II,* Edward Elgar, pp. 569-596.

Shavell, S. (1987), *Economic Analysis of Accident Law,* Harvard University Press.

Seng, D. (2015), “Who watches the watchmen?” An Empirical Analysis of Errors in DMCA Takedown Notices, available on SSRN ID 2563202.

Spence, A.M. (1975), “Monopoly, Quality, and Regulation”, The Bell Journal of Economics, 6, pp. 417-429.

Trimble, M. and Mehra, S.K. (2014), “Secondary Liability, ISP Immunity, and Incumbent Entrenchment”, The American Journal of Comparative Law, 62, pp. 685-706.

Ulys (2006), *Liability of the Internet intermediaries*, Study for the European Commission.

Urban, J.M, J. Karaganis and B.L. Schofield (2017a), “Notice and Takedown: Online service provider and rightholder accounts of everyday practices”, Journal of Copyright Society 64, pp. 371-410.

Urban J.M, B.L. Schofield and J. Karaganis (2017b), “Takedown in Two Worlds: An Empirical Analysis”, Journal of Copyright Society, 64, pp. 483-520.

cerre

Centre on Regulation in Europe

Avenue Louise, 475 (box 10)
1050 Brussels, Belgium

+32 2 230 83 60

info@cerre.eu

cerre.eu

@CERRE_ThinkTank