Rethinking liability rules for online hosting platforms

Buiten , Miriam; De Streel, Alexandre; Peitz, Martin

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Discussion Paper Series – CRC TR 224

Discussion Paper No. 074
Project B 05

Rethinking Liability Rules for Online Hosting Platforms

Miriam Buiten*
Alexandre de Streel**
Martin Peitz***

March 2019

*University of Mannheim, MaCCI
**University of Namur, CRIDS/NADI and CERRE
***University of Mannheim, MaCCI, CERRE

Funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) through CRC TR 224 is gratefully acknowledged.

Rethinking Liability Rules for Online Hosting Platforms

Miriam Buiten, *University of Mannheim, MaCCI*

Alexandre de Streel, *University of Namur, CRIDS/NADI and CERRE*

Martin Peitz, *University of Mannheim, MaCCI, CERRE*[1]

Abstract

With the growing economic and societal importance of online platforms, the question of their liability for illegal content or products they host becomes more important. Based on an analysis of platforms' incentives, we address the appropriate liability rule for hosting service providers and derive policy recommendations for an efficient liability regime in the European Union. Online hosting platforms may take monitoring efforts on their own initiative that are suboptimal due to the presence of externalities and asymmetric information problems, warranting some form of liability rules. However, for more fundamental reasons of free speech and preventing censorship, policy makers may want to be cautious in entrusting – and burdening – private parties which such an extensive 'policing' role. Additionally, higher monitoring requirements may disproportionally burden small entrants. As we argue, since several actors participate to the diffusion of illegal material online, the responsibility of a safe Internet should be shared among all these actors. Concrete regulatory improvements may encourage online hosting platforms to do their part in monitoring proactively and diligently, such as affirming a good Samaritan clause.

Keywords

Online platforms, illegal content, e-commerce, liability rules

[1] The authors are grateful to the helpful comments by participants of the CERRE Executive seminar on platform liability, the Hamburg Lectures series in Law and Economics, the LawEcon Workshop in Bonn and the Mannheim Workshop on Governance of Platform Markets in the Big Data era. This article is based on de Streel, Buiten and Peitz (2018), a study written for the Centre on Regulation in Europe (CERRE, www.cerre.eu). The study and this article reflect the views of the authors only; it may not reflect the view of CERRE members. Miriam Buiten and Martin Peitz gratefully acknowledge financial support from Deutsche Forschungsgemeinschaft (DFG) through CRC TR 224.

1. Introduction

Online hosting platforms have matured and gained economic and societal importance in the last decade. Hosting platforms have evolved from passively displaying offers to sophisticated players that govern which users can participate, what information users obtain, and how transactions are made. Today's platforms, from Facebook to Twitter and from Uber to Ebay, regulate users' access to platforms as well as police and regulate their behaviour and expression on their platforms. Some hosting platforms have emerged as central facilitators in the internet economy, such as Amazon for e-commerce.

With this central role of hosting platforms in the digital economy, a natural question to ask is what their responsibility ought to be for illegal content or products hosted on their platforms. Currently, the e-commerce Directive exempts hosting platforms from liability for illegal material, as long as they provide a service of a passive nature and remove illegal material expeditiously upon obtaining knowledge of it. The question is whether this exemption rule that helped hosting platforms flourish at their inception twenty years ago is still appropriate for today's hosting platforms.

Hosting platforms do take voluntary initiatives to combat illegal material. Amazon, for instance, rolled out a program in which it cooperates with brands to place unique barcodes on each product, in order to detect and remove counterfeit products from its site.[2] It has an in-house team to take action on reported violations and has invested in machine learning and automated systems to detect copyright violations. Nevertheless, when facing lawsuits Amazon maintains that it is not liable for counterfeit goods sold on its site because it is a platform for sellers, rather than a seller itself.[3] It could be questioned if this is appropriate in cases where third-party counterfeits were sold using the "Fulfilled by Amazon" service, meaning that Amazon took care of the entire transaction including storage, shipping and payment processing.

Against this background, this paper considers the appropriate liability rule for hosting service providers. Taking an effects-based perspective, we aim to derive policy recommendations for an efficient EU liability regime.

We find that given the incentives and costs of hosting platforms to monitor, a negligence-based system for hosting platforms would be the preferred approach. Hosting platforms may take suboptimal monitoring efforts on their own initiative due to the presence of externalities and asymmetric information problems. Whereas the current legal framework exempts hosting platforms from liability, it only does so under certain conditions. We propose several concrete improvements to these conditions, to ensure that hosting platforms do their part in preventing harm from illegal, unwanted and dangerous material. Such improvements include the confirmation of a clear Good Samaritan clause and the requirement of transparent procedures for counter-notice in hosting platforms' notice-and-takedown systems. More generally, the legal framework should encourage all parties involved to do their part in preventing illegal material. On the part of hosting platforms, this includes providing an effective infrastructure allowing efficient detection and removal of illegal material.

The paper proceeds as follows. Section 2 of the paper considers the rules and the objectives of the e-commerce Directive adopted in 2000 and the regulatory evolution afterwards. Section 3 analyses the

[2] Masters, K. (Forbes, 3 January 2019) "The Amazon Transparency Program Is A Counterfeiter's Worst Nightmare", <https://www.forbes.com/sites/kirimasters/2019/01/03/the-amazon-transparency-program-is-a-counterfeiters-worst-nightmare/>m last visited 15 February 2019.

[3] Semuels, A. (The Atlantic, 20 April 2018) "Amazon May Have a Counterfeit Problem", < https://www.theatlantic.com/technology/archive/2018/04/amazon-may-have-a-counterfeit-problem/558482/>, last visited 29 January 2019.

incentives of the platforms, their users and third parties to detect and remove illegal and dangerous material. It shows that these private incentives do not always match the public interest, implying that liability rules need to be introduced. Section 4 offers recommendations for an appropriate liability regime and Section 5 concludes.

2. The evolution of the liability rules for online hosting platforms

2.1. The origin: the limited liability regime of the e-commerce Directive

In 2000, when Internet hosting platforms were in their infancy, the e-commerce Directive[4] established a special liability regime for the hosting services based on four pillars.

The first pillar sets the *country of origin principle* to strengthen the internal market.[5] It implies an Internet hosting platform is only subject to the liability regime of the EU member state where it is established.

The second pillar creates an *exemption from the national liability regime* to which the hosting platform is subject to and harmonises at the EU level the conditions for such exemption[6]. A hosting platform can escape liability for illegal material when it does not have knowledge of the illegality or, upon obtaining such knowledge, it acts expeditiously to remove or disable the access to the material (notice-and-takedown). The Court of Justice of the European Union has interpreted these conditions by distinguishing between, on the one hand, services that are purely passive and neutral, which can benefit from the liability exemption and, on the other hand, services that are more active and cannot benefit from the exemption.[7]

The third pillar is the *prohibition for EU member states to impose a general obligation on the hosting platforms to monitor* the material hosted.[8] The Court of Justice of the EU has drawn a blurred line between general monitoring measures, which are prohibited, and specific monitoring measures, in particular in case of suspected violation of intellectual property rights, which are allowed.[9]

The fourth pillar is the *encouragement of co- and self-regulation* to implement the rules and principles of the directive.[10]

As explained by the European Commission (1998), this legal regime pursues four main objectives. (i) The first was to share responsibility for a safe Internet between all the private actors involved and a good cooperation with public authorities. Thus, the victims should notify the hosting platforms on any illegality they observe and the hosting platforms 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. (ii) The second objective was to encourage the development of e-commerce by increasing legal certainty on the role of each actor and by ensuring that the hosting

[4] 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.

[5] Article 3 of the e-commerce Directive.

[6] Article 14 of the e-commerce Directive.

[7] Cases C-236/08 to C-238/08 *Google France v Louis Vuitton*, EU:C:2010:159; Case C-324/09, *L'Oreal et al. v. eBay*, EU:C:2011:474, points 115-116 ; Case C-484/14 *Mc Fadden*, ECLI:EU:C:2016:689, para 62. Those cases are well explained in Husovec (2017), Nordemann (2018) and Van Ecke (2011).

[8] Article 15 of the e-commerce Directive.

[9] Case C-360/10 *SABAM v. Netlog,* EU:C:2012:85; Case C-70/10 *Scarlet Extended v. SABAM*, EU:C:2011:771; Case C-31412 *UPC Telekabel Wien*, EU:C:2014:192.

[10] Article 16 of the e-commerce Directive.

platforms do not have an obligation to monitor the legality of all material they store. This would have been extremely costly, especially at a time when machine-learning based technologies were very nascent. (iii) The third objective was to strike a fair balance between different fundamental rights, in particular privacy and the protection of personal data, the freedom of expression and information, the freedom to conduct business and the right to property including intellectual property.[11] (iv) The fourth objective was to strengthen the digital single market by adopting a common EU standard for a liability exemption, especially at a time when national rules and case law were increasingly divergent.

2.2. The evolution: towards a differentiated liability regime

Since the adoption of the e-commerce Directive in 2000, technology and markets have changed dramatically. Online platforms are offering new types of services with the development of web 2.0 relying on user-generated content or the progress of the collaborative economy blurring the lines between producers and consumers. Now, the users, but also the platforms, play a more active role and the criteria set by the Directive and the Court of Justice to benefit from the liability exemption are more difficult to apply. Moreover, some online platforms have become very large. This is often attributed to direct and indirect network effects, which can be partly due to data-driven feedback loops.[12] As a result, the harm caused by illegal material is more massive while their financial, technological and human capacities to prevent and remove such illegal material have expanded. Moreover, more effective machine-learning based techniques for identifying illegal content have become available, decreasing the costs for victims and online hosting platforms to prevent harm caused by illegal material.

These evolutions triggered a call to increase the responsibility of the online platforms (European Commission, 2016). Responding to this call the EU institutions did not change the four pillars of the e-commerce Directive but clarified some of its provisions in order to step-up the fight against illegal material and, in parallel, developed stricter specific rules for some types of material which are particularly harmful (as summarised in Table 1 below).

First, the Commission clarified the e-commerce Directive by adopting a Communication in 2017, followed by a Recommendation in 2018.[13] These two instruments aim to improve the effectiveness and transparency of the notice-and-takedown process between the victims and the platforms, stimulate proactive measures by online platforms, and increase cooperation between providers of hosting services and the other stakeholders (in particular of users, trusted flaggers and public authorities). Yet, the legal effects of these instruments is not entirely clear as it is not obvious that all the principles of the Communication and the Recommendation directly stem from the Directive and could be made binding on the basis of the Directive.

Secondly, the baseline regime of the e-commerce Directive has been complemented for particularly harmful illegal material by sectoral rules and co/self-regulatiory. measures Thus, the online diffusion of child sexual abuses is now prohibited by a specific directive[14] and multiple commitments have been

[11] As protected by resp. Articles 7 and 8, 11, 16 and 17 of the Charter of Fundamental Rights of the European Union.
[12] Belleflamme and Peitz (2015); Martens (2016).
[13] Communication of the Commission of 28 September 2017, Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms, COM (2017) 555 and Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, O.J. [2018] L63/50. Although Recommendations and Communications are soft-law instruments, the legal value of the former is slightly higher than the former.
[14] 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.

taken by digital firms to fight such propagation.[15] Similarly, the online diffusion of terrorist content has been prohibited by specific legislation[16] and a Multi-Stakeholders Forum has been set up between the Internet platforms and the enforcement agencies to reduce such diffusion.[17] The online diffusion of hate speech is now subject to the revised Audiovisual Service Media Directive[18] and a Code of Conduct has been adopted to reduce such propagation.[19] 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 violations on the Internet[20] 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. [21]

Table 1: EU rules against online illegal material

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 - Prop. Reg. terrorism online content	- Rec. 2018/334 Illegal content online	- EU Internet Forum (2015)
Hate speech	- Dir. 2010/13 Audiovisual Media Services as modified by Dir. 2018/1808 in case of video-sharing platforms		- CoC Illegal hate speech online (2016)
IP violation – copyrighted content	- Prop Dir. Copyright in the Digital Single Market		
IP violation – counterfeit goods			- MoU Counterfeit goods online (2011-2016)

[15] Several initiatives were established to fight the diffusion of child sexual abuses online: a CEO Coalition in 2011: https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kid (last visited 26 February 2019); an ICT Coalition for Children Online in 2012: http://www.ictcoalition.eu (last visited 26 February 2019); and an Industry Alliance to deal with child sexual abuses in 2017; https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online (last visited 26 February 2019).

[16] Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, O.J. [2017] L 88/6; Proposal of the Commission of 12 September 2018 for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, COM(2018) 640.

[17] An EU Internet Forum was established in 2015: Commission Press release of 3 December 2015, IP/15/6243.

[18] Article 28a of the amended 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 EU member states concerning the provision of audiovisual media services in view of changing market realities.

[19] Code of Conduct of 31 May 2016 of countering illegal hate speech online <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300> last visited 23 February 2019.

[20] 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.

[21] Revised Memorandum of Understanding of 21 June 2016 on the sale of counterfeit goods via Internet.

These reforms, despite their usefulness, have not halted the debate on the responsibility of hosting platforms. 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, we evaluate the appropriate liability for online platforms from an effects-based perspective.

3. Designing efficient liability rules for online hosting platforms

3.1. The role of online hosting platforms

Hosting platforms can be described as intermediaries that seek to facilitate interaction between different user groups (e.g., Hagiu and Wright, 2015). In their role as an intermediary, hosting platforms provide governance. They provide access restrictions for using the platform as well as conduct restrictions on the platform, aiming to secure the safety on the platform.

When hosting platforms fail to prevent the occurrence of harm on the platform, it stands to reason that they face some form of liability. This is notwithstanding the liability of direct tortfeasors, such as sellers of counterfeit goods on an online marketplace. Surely, harm on hosting platforms would decrease if fewer sellers would offer counterfeits. Liability rules should be in place to discourage this illegal activity. Nevertheless, hosting platforms have a role to play too in minimizing harm. Hosting platforms reap the benefits of exchange on the platform. They should therefore bear the costs, in the form of harm of illegal material, associated with the exchange they facilitate. In other words, hosting platforms should contribute to internalizing the negative externality caused by their business model. Moreover, by imposing rules of participation, the hosting platform regulates exchange. Consequently, it carries responsibility for the environment it governs, analogous to fiduciary duties of financial intermediaries.

The more involved the hosting platform is in the activities on the platform, the more may be expected from the platform in terms of monitoring and preventing harm. Insofar as a hosting platform enjoys more profits as the platform carries less illegal material, the hosting platform has an interest in preventing the illegal material on their own. This is clearly not the case for hosting platforms whose business model revolves around the exchange of illegal material, such as websites hosting pirated movies. However, even legitimate hosting platforms' incentives to monitor and remove illegal material may not be socially optimal. Not all the harm caused by illegal material may hurt the business or reputation of hosting platforms. Given that detecting and removing illegal material is costly, hosting platforms may not take sufficient measures to prevent it. Consequently, when other parties suffer harm, a liability rule may be necessary to induce online hosting platforms to detect and remove illegal content.

Overall, determining the appropriate liability rule for online hosting platforms requires evaluating their incentives to detect and remove illegal material. Given the costs of monitoring, an efficient liability rule does not aim at eliminating illegal material altogether. Instead, a liability rule should be designed to minimize the combined costs of both harm and of detection and removal.[22] Insofar the private costs and benefits of detecting and removing harm of online hosting platforms coincide with the social costs, online hosting platforms can be expected to spend a socially optimal level of effort on monitoring and removing illegal material. Otherwise, privately and socially optimal levels differ.

Online hosting platforms are not the only actors able to reduce the costs of harm from illegal material. It may be the case that another party, such as users or third party-victims has better information available to detect harm. In such cases, however, the online hosting platform may still need to get

[22] According to the economic analysis of liability rules (Calabresi, 1970; Landes and Posner, 1987; Shavell, 1987), liability rules should aim at minimising costs of harm that result from activities or transactions.

involved in order to remove the harm. In short, determining the appropriate liability for online hosting platforms requires comparing the costs and benefits of all actors involved in illegal material on online platforms, and consequently their private incentives to detect and remove such material. In the following, we consider the incentives of online hosting platforms, platform users and third parties.

3.2. Incentives of online hosting platforms

3.2.1. Harm suffered by online hosting platforms

A first type of harm to the online hosting platform may be a *reduction in customers' participation or activity level* on the platform, as a result of deteriorated user experience. Sellers offering illegal material may attempt to mislead or defraud users, which may discourage users from using the hosting platform's services. The hosting platform risks losing users to competitors that offer content that is more trustworthy or products, or information that is more accurate. In addition to losing customers, the hosting platform may also face reduced activity on its platform. Even a monopoly hosting platform 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, p. 13).

A second type of harm for online hosting platforms may be to their *reputation*. In the long term, the presence of illegal content, goods or services on the hosting platform's platform may harm its credibility and reputation.[23] The hosting platform 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 hosting platform.

A third force driving hosting platforms to take down illegal material may be the *prevention of regulation* itself (Husovec, 2017). Hosting platforms 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 hosting platforms.

Alongside these considerations based on profit-maximising incentives, hosting platforms may be committed to nurturing a healthy community or encouraging creative or innovative offers by their providers as a goal by itself. 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,p. 13), as this affects their attractiveness to employees and investors.

3.2.2 Costs of prevention for online hosting platforms

A hosting platform 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 enforce a minimum quality standard and punish misbehaving or underperforming users by banning them from the platform. Uber, for instance, deactivates drivers if they receive bad user reviews or if they violate company policy.[24]

[23] See also Kraakman (1986, p.56) on reputational concerns and contractual arrangements driving private enforcement.

[24] Avery Hartmans, "10 ways Uber drivers can get kicked off the app", Business Insider (23 July 2017), <www.businessinsider.com/how-uber-drivers-get-deactivated-2017-7> (last visited 10 December 2018).

If the hosting platform can influence the behaviour of its users or limit the resulting harm, it is likely costly for the hosting platform to deploy the measures at its disposal. The associated costs include costs to develop detection software, as well as costs of maintaining review systems and notice and takedown systems, including responding to users' notices. The development of detection software can be considered a proactive measure allowing online hosting platforms to become aware of and find the illegal content. Online hosting platforms may also exert effort to, subsequently, remove or limit access to illegal information or illegal goods or services from a platform. This includes measures against violators, such as hosting platforms' efforts to filter content in order to prevent illegal behaviour of users, or excluding violators from the platform altogether (Sartor, 2017, p. 10).

Several considerations may affect the extent of detection and removal costs of online hosting platforms. The costs of detecting illegal material and of removing it may vary depending on (1) the size of the platform, (2) the type of harmed party, (3) the hosting platform's business model and (4) the type of illegal material.

(1) First, the *size of the platform* may affect hosting platforms' 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 hosting platforms, with more activity or transactions on their platform, likely deal with more instances of illegal material than small hosting platforms 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 hosting platforms may benefit from economies of scale. Because of their larger number of transactions, it may pay off for large hosting platforms to invest in developing or acquiring software tools to identify and filter out illegal content. Large hosting platforms can spread the high fixed costs of such software tools over all instances of illegal material, and cover it with their higher revenues. Moreover, 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 hosting platforms, 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 hosting platforms. As a possible downside, this may discourage socially beneficial business activity of hosting platforms as it increases the cost of operation. If the costs to comply with the duty of care are significantly higher for small hosting platforms than for large ones, the liability rule may make doing business too costly for small hosting platforms. Large incumbents obtain an advantage as compared to small competitors, potential entrants may be discouraged from entering the market and small hosting platforms 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 hosting platforms 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.

(2) 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 hosting platform and is in a

position to do so. If this is the case, the hosting platform may be able to rely largely on responding to notifications, rather than having to engage in active monitoring. We return to this point below when discussing the incentives of users and third parties to detect and remove illegal material.

(3) Thirdly, the *business model of the hosting platform* 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 or copyright holders provide them with notifications to remove the illegal goods or content 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.

(4) 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 more and more precise control[25]. 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.[26] 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.[27] 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.[28]

3.2.3 Errors in detecting illegal material

Even in areas where detection software is available, they are prone to errors. 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, p. 42).[29] When removing material using automated tools, online hosting platforms 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

[25] For an overview of those techniques to detect copyrighted material, see Annex 12 of the Commission Impact Assessment on the Proposal for a Directive on copyright in the Digital Single Market, SWD(2016) 301.

[26] "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/ (last visited 23 February 2019).

[27] Regarding some illegal content, determining illegality may require specific case-by-case review, such as in cases of hate speech or terrorist content. The hosting platform 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 hosting platforms might need to rely more on manual detection by humans in order to detect and remove content, which tends to raise precaution costs.

[28] Even if online hosting platforms can rely on notifications by users for some types of material, such as fraud on trading platforms, maintaining such a notice and takedown system is likely to be costly. Therefore, the availability and development of automated tools to detect illegal material may reduce precaution costs of online hosting platforms.

[29] See further Seng (2015).

by the online hosting platform (Trimble and Mehra, 2014). The online hosting platform 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 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 hosting platform 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, p. 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 hosting platforms to pre-emptively evaluate material that users put online (Doctorow, 2008, p. 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, p. 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, p. 42). A fundamental public policy question is to what extent society wants to entrust – and burden – private parties with such a "policing" role (See e.g. Belli et al., 2017). Considering the substantial effects of hosting platforms' decisions on notices, some find that online hosting platforms weld an inordinate amount of gatekeeping power in notice and takedown regimes (Logan, 2016, p.38-39). Notice and takedown systems resulting in censorship, limitations to free speech and to other fundamental rights may provide an argument against liability of online hosting platforms 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.

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 hosting platform'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 hosting platforms when liability depends on the knowledge of illegal material of the online hosting platform. If the automated content removal system has considered certain material and incorrectly found it to be legal, the online hosting platform 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 hosting platform may be inclined to remove too much, rather than too little material.

3.3. Incentives of users and third parties

3.3.1. Harm suffered by users and third parties

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* 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 (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, for instance when faced with harmful products or content such as malware. Similarly, providers may lose the benefits of transactions they engage in with buyers or users in cases of non-payment.

Cases of harm within the contracting relationship often have spill over effects on *third parties*. Take the case of outright fraud on an online hosting platform. 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 hosting platform may suffer from the presence of fraudsters on the platform.

Third parties may also be harmed directly by the activities taking place on online platforms. Users may suffer harm as a third party, for instance when they 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.[30] 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 hosting platform hosting this content. A user suffers discrimination because information is available to the user engaging in discrimination.[31] Nevertheless, in such cases, the online hosting platform may suffer indirect harm as well.

Another group of third parties that may suffer harm consists of *intellectual property right holders*. For instance, if counterfeit products are offered on an online platform or copyrighted material is illegally sold by someone else than the right holder, the right holder suffers harm. Some right holders might be in a position to leverage their business relationships to induce online hosting platforms to take action against illegal material. They may threaten to leave the platform if the hosting platform does not act against the sellers of the counterfeited goods.[32]

Broader groups of victims may suffer harm from producing, creating or providing the products, content or services. For instance, individuals who are the victim of certain hate speech may be users of the online platform, 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 society or aid in the preparation of terrorist activities. Yet other examples are malware and malfunctioning products: 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.

3.3.2. Costs of prevention for users and third parties

The possibilities for injured parties to take precautionary measures vary considerably depending on the type of injured party, type of illegal material and type of harm. Buyers and sellers in some cases

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

[31] 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.

[32] For example, as reported in German media, the German shoe producer Birkenstock stopped selling via Amazon from January 2018 claiming that Amazon did not take sufficient measures against counterfeits. See <www.spiegel.de/wirtschaft/unternehmen/birkenstock-legt-sich-mit-amazon-an-a-1182571.html> (last visited 26 February 2019).

may be able to reduce the risk of harm by obtaining more information about the counterparty, for instance relying on online hosting platforms' 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 hosting platform, 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 hosting platform). 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 (e.g. illegal trade in exotic animals). In cases of very serious harm, such as child pornography material, 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 hosting platforms about infringements so that the content can be removed. In some cases, right holders may have leverage with hosting platforms 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, 2017).

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 hosting platform of the harmful content, so that it can be removed (see further subsection (b) below).

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 hosting platforms. 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, 2017). For instance, the users engaging in the illegal behaviour may be anonymous or not easily reachable (Sartor, 2017, p. 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. Enforcement costs are likely to be higher if the defendant is located in another country. Online hosting platforms allow for transactions with strangers 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.

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 hosting platform. Particularly in cases of terrorist

content, no individual may take action to notify the hosting platform, let alone have the means available to reduce the harm of terrorist content in other ways.

3.4. Interdependence of the incentives of the online hosting platforms, their users and third-parties

In cases in which users or other injured parties have the information to detect illegal material, the online hosting platform may still need to play a role. Users and particularly third parties may have no means available to remove the illegal material once they have detected it. They often depend on the online platform to do so. For instance, even when a seller finds out that products he has been selling are counterfeit and wants to stop selling them, he may need the cooperation of the platform to take down the offer. In short, the costs of detecting and removing illegal material for users of the platform are linked to the infrastructure for doing so offered by the online hosting platform.

This distinguishes the case of illegal material on an online platform from a standard, two-party transaction. Instead of comparing who is best place to detect and act on an illegality, we need to consider how efforts of one party (the online hosting platform) may facilitate action by others (the users).

Online hosting platforms can enable users to contribute to removing illegal material through their rating systems and their notice- and takedown systems. An effective rating or reputation system may affect incentives on both the provider side and the user side. Such a system enables users to weed out illegitimate sellers on an e-commerce platform. This, in turn, disciplines providers who know that illegal activities may cost them their reputation on the platform. In this way, online hosting platforms can help preventing harm from illegal material from simply allowing users to share their experiences among each other. A user-friendly notice- and takedown system can allow users that have information on illegal material to share it with the platform, so that the platform can take action.

There is one caveat to this solution: it only works if the platform is interested in removing the illegal material. There may be cases in which the online platform aims to enable a conspiracy between the participants of the platform. One could think of online platforms dealing with illegal exchanges in the "dark web", or hosting platforms focused solely on allowing the illegal exchange of copyrighted materials or counterfeited goods. In such cases, where a negative externality is at play, the platform has no incentive to intervene. This provides a clear rationale for legal rules (in the form of civil liability or otherwise). Many platforms, however, are not complicit in providing the illegal material but are unaware of it. In such cases of asymmetric information, the online hosting platform likely wants to mitigate the market failure because of the threat of losing business or users. Arguably, the rise of online hosting platforms is closely linked to their success in reducing asymmetric information problems (Belleflamme and Peitz, 2018).

Offering reputation systems is a way to mitigate the asymmetric information problem. An online hosting platform can act on behalf of the prospective buyer to reduce the latter's information disadvantage vis-à-vis the seller, as discussed above. Market power of the online hosting platform 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 hosting platform can remove the seller from the platform, the seller may be discouraged from exploiting the buyer; thus, the hosting platform mitigates the associated moral hazard problem of the seller. By removing or downgrading the seller, the hosting platform may also mitigate adverse selection resulting from different abilities of sellers in providing adequate content. By mitigating asymmetric information problems, online hosting platforms may facilitate the functioning of markets that would otherwise fully

or partially break down. For instance, transactions taking place on Ebay, Uber and Airbnb may not take place if it were not for an online hosting platform creating an environment of trust between providers and users on their platform.

The incentives of the hosting platform to act in this beneficial way may depend on the monetisation instrument it uses. If the hosting platform 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.[33] The hosting platform, in this case, will primarily be interested in collecting fees from the sellers and, thus, focus on seller surplus. When positive indirect network effects are present, consumer benefits still matter to the hosting platform 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. Moreover, technological developments have allowed hosting platforms to better monitor transactions and monetise them. This suggests that extending liability for hosting platforms may not be a priority for policy, because hosting platforms 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, hosting platforms are less likely to act in the best interest of this group of users.

An effective liability regime recognizes the interdependence between incentives of users and incentives of online hosting platforms for detecting and removing illegal material. In order to induce all parties involved to 'do their part', the online hosting platform may need to be required to implement an effective infrastructure for its reputation system and notice- and takedown system.

Beyond this structural requirement, a liability rule may be imposed for illegal material hosted by online hosting platforms. Such a liability rule would need to balance not only the costs of detection and removal for online hosting platforms, but also the potential benefits of their activities. Aside from those online hosting platforms focusing primarily on illegal material, for the most part, hosting platforms enable socially beneficial activities. Ideally, the liability system does not discourage these socially beneficial activities. To the extent that liability would induce hosting platforms to abandon or limit their services, liability would negatively affect not only the hosting platforms, but also the users of the hosting platforms' services. In particular, business models in which services or content are provided for free may not be sustainable when hosting platforms are subjected to liability, since revenues may not cover the expected damages payments (Sartor 2017, p. 11).

Finally, online hosting platforms 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, p. 1). Liability for illegal content would, in many cases, require online hosting platforms to make judgment calls regarding the content they host. This, in turn, raises concerns regarding censorship and discrimination. It also raises concerns about inhibiting entry by providers of products and services.

3.5. Efficient liability of hosting platforms

To summarise, an efficient liability of hosting platforms should minimise the costs of harm that result from activities or transactions on these platforms. Three key elements should be borne in mind when designing liability rules for hosting platforms.

[33] An example of a hosting platform charging only listing fees are Yellow Pages, which do not monitor or benefit from the transactions on its platform.

First, *multiple parties* are involved on hosting platforms that can contribute to preventing harm. In many cases, *hosting platforms* are best placed to monitor and control the behaviour of users and subsequently reduce the expected harm, making some form of liability for hosting platforms appropriate. Hosting platforms may well be interested in monitoring on their own initiative. Insofar this is the case, the duty of care does not significantly change their monitoring efforts and the policy intervention may be almost neutral. Insofar as hosting platforms do not engage in cost-effective monitoring on their own initiative, liability rules are necessary and help induce these hosting platforms to take measures to reduce the costs of harm. Nevertheless, *injured parties* should also be encouraged to do their part in prevention and detection of harm. Hosting platforms can enable users to contribute to removing illegal material through their rating systems and their notice- and takedown systems. In short, an efficient liability system encourages both hosting platforms and users to help reduce harm.

Second, liability rules should not merely encourage hosting platforms to monitor and remove illegal material, but also to do so *diligently while minimising errors*. A one-sided liability for failure to remove illegal material may result in over-removal by hosting platforms, with dire consequences for users' business interests and citizens' access to information. More nuanced rules or guidelines should induce hosting platforms to improve the accuracy of notice- and takedown systems.

Third, there is *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 type of illegal material and the type of harm. For instance, hosting platforms may need a stricter duty of care for severe types of harm where victims are dispersed, such as terrorist content and child sexual abuse material. Similarly, victims of illegal hate speech may have limited means to enforce their rights and may need to rely on effective notice- and takedown systems.

4. Policy recommendations

4.1. A revolution: EU harmonisation of the liability rules of providers of hosting services

On the basis of the incentives and costs of hosting platforms to monitor for illegal material, 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 hosting platforms 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 (Sartor, 2017). In the specific case of secondary liability of online hosting platforms for copyright violations, Nordermann (2018) recommends the introduction of liability rules at the EU level in order to create a level playing field in the digital single market. To be sure, 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 EU member states would have to be considered when creating specific liability rules at the EU level for specific types of claims.

However, due to political economy considerations, an EU harmonisation of the national rules for secondary liability of online hosting platforms 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 at the core 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,[34] 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 (for instance, Husovec, 2017; Nordermann, 2018; Sartor, 2017; Van Eecke, 2011) does not call for fundamental overruling of the e-commerce Directive but only for adaptations.

4.2. An evolution: linking the EU liability exemption to the provision of an infrastructure facilitating detection and removal of illegal material

In this light, we present a solution consisting of maintaining the current exemption system with improvements to ensure, following Helberger et al. (2018, p. 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 and the size of hosting providers. Many features of this infrastructure are already mentioned in the Commission Communication of September 2017 and in the Commission Recommendation of March 2018 on measures to effectively tackle illegal content online.[35] An exemption for start-ups is worth considering. This may help startups because entry costs due to necessary investment are likely to go down. However, their reputational costs may go up.

4.2.1. 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). This implies that the possible current dis-incentive to use proactive measures possibly caused 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.[36] Even if the hosting platform may not take down all illegal material it detects through its own active monitoring efforts, this outcome is still preferable to the hosting platform not engaging in these active monitoring efforts altogether. It is moreover important for the development of the technologies that online hosting platforms are not penalised for their voluntary implementation of content identification

[34] 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.

[35] Some characteristics are also mentioned in the new Article 28a of the revised Audiovisual Media Services Directive and Article 13 of the new Directive on copyright in the Digital Single Market. However, our proposal is more modest than the AVMS Directive because we propose to condition the liability exemption to the provision of measures for effective detection and removal of illegal content but we do not propose to impose those measures.

[36] Also in this sense, Sartor (2017, p. 29). Note that 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. In a liability system without a Good Samaritan clause, hosting platforms may refrain from voluntary monitoring efforts, because these efforts would lead the hosting platform to find more illegal material, which in turn would pose liability risks on them. A Good Samaritan clause should aid platforms when taking voluntary measures, by removing the risk of being sanctioned for under-removal.

technologies (Trimble and Mehra, 2014, p. 693). At the same time, 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 and those mechanisms should be clearly communicated to the users. Second, effective rating or reputation mechanisms should be encouraged when relevant to decrease the asymmetry of information suffered by the users of the platforms.

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 hosting platforms or users should be encouraged as an effective detection means, provided some safeguards be 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 (European Commission, 2018). However, stakeholders and authorities should set 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 product is removed after an automated detection;[37] (iii) third, the need to share these technologies between large hosting platforms, which have the data, the expertise and the financial means to develop automated techniques, and the small or new hosting platforms.[38]

4.2.2. 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 serious and quickly inflicted and/or when the illegality is notified by an enforcement authority or a trusted flagger.

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.

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.

[37] Similarly to what is imposed by Article 22(1) of the Data Protection Regulation in case decision solely based on an automated processing of personal data: Malgieri and Commandé (2017).

[38] This is the case Microsoft' Photo DNA fighting the diffusion of child abuse material: <https://news.microsoft.com/en-gb/2013/11/18/tacklingproliferatio/> (last visited 26 February 2019).

4.2.3. The differentiation of care

An 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, the level of care for the platforms should be higher for material that may cause particularly serious harm, or harm across a dispersed group of victims. For instance, for terrorism content, the Commission Recommendation of March 2018 already provides for a stricter duty of care and a specific Regulation is now being negotiated. 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.

For types of harm that affects users or consumers who have the ability and 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. 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.

Therefore, we suggest complementing these reforms related to the baseline liability regime applicable to all types of illegal material with effective co-regulatory measures for specific types of material where additional care is required. Thus, for the types of material that 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. General principles for the liability framework

More generally, the regulatory framework to tackle illegal material on the Internet should be guided by the following good regulatory principles. First, the presence of illegal material on the Internet involves many actors (providers of material, platforms, victims, public authorities, etc.). Hence, 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 responsibility. For this reason, two extreme solutions should typically be avoided when determining the liability of online hosting platforms: a full liability exemption and strict liability. A full liability exemption is problematic, because hosting platforms should be induced to cooperate to the detection and the removal of illegal activities on the Internet. Shielding online hosting platforms from all liability if they do not cooperate would not contribute to this goal. A strict liability rule, by contrast, shifts a considerable burden of 'policing the Internet' on online hosting platforms – more than we may want to, given concerns of censorship and access to information.

Second, *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 then be clarified by the European Commission in delegated or implementing acts or interpretative guidance, which are easy to adopt and change in light of technology and market evolutions. In particular, guidance prevents that the liability rules remain vague, and ensures that online hosting platforms have the necessary knowledge and legal certainty to fulfil their obligations and responsibilities.

Third, the liability hard-law 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.

5. Conclusion

We considered if and how the growing economic and societal importance of online hosting platforms ought to affect their liability when hosting illegal material. When we abstract from the regulatory status quo, the incentives and costs of hosting platforms to monitor for illegal material suggests that a negligence-based system would be 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 hosting platforms, this in practice does not give online hosting platforms 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 hosting platforms 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 hosting platforms' notice-and-takedown systems. Overall, EU rules should incentivise hosting platforms 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 provided some general guidance to policy makers in improving the regulatory framework regarding online hosting platform liability. First, the liability 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. Second, the liability rules of online hosting platforms should be principles-based to be easily adaptable to technology and business models, which evolve quickly and often in unpredictable ways. Third, a promising option is that liability rules be complemented with co-regulation or self-regulation such as codes of conduct.

References

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, pp. 215-254.

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.

de Streel, A., M. Buiten, and M. Peitz (2018), Liability of Online Hosting Platforms: Should exceptionalism end? CERRE Report, September 13, 2018.

Edelman, B., Luca, M., & Svirsky, D. (2017). Racial discrimination in the sharing economy: Evidence from a field experiment. American Economic Journal: Applied Economics, 9(2), 1-22.

European Commission (1998), Explanatory Memorandum of the Commission proposal for a directive on certain legal aspects of electronic commerce in the internal market, COM(1998) 586.

European Commission (2016), Communication of 25 May 2016 on online platforms and the Digital Single Market, COM(2016) 288.

European Commission (2018), Communication of 25 April 2018, Artificial Intelligence for Europe, COM(2018) 237.

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

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

Hagiu, A. and J. Wright (2015), "Multi-Sided Platforms", *International Journal of Industrial Organization* 43, pp. 162-174.

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

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

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.

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

Malgieri G. and G. Commandé (2017), "Why a right to legibility of automated decision-making exists in the General Data Protection Regulation", *International Data Privacy Law* 7(4), pp. 243-265.

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

Nordemann, 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.

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.

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

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

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

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.

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.

Van Eecke P. (2011), 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review* 48, pp. 1455-1502.