
Reform of the EU liability regime for online intermediaries

Background on the
forthcoming
digital services act



IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service

Author: Tambiama Madiaga
Members' Research Service
PE 649.404 – May 2020

The E-commerce Directive, adopted in 2000, aims at harmonising minimum standards of liability for internet (online) intermediaries across the European Union (EU). Under the current EU legal framework, digital or online platforms are not legally responsible for hosting illegal content, but are required to remove such material once it is flagged. However, technologies and business models have evolved in the last 20 years and the EU liability framework struggles to capture liability issues raised by new actors, such as search engines, social networks and online marketplaces. Furthermore, societal challenges have changed the nature and scale of liability, with the development of a range of new harmful online practices, such as the dissemination of terrorist content online, the increasing use of platforms to distribute counterfeit products and the spreading of false or misleading news and online advertisements. The European Commission has pledged to present a new framework to increase and harmonise the responsibilities of online platforms. New EU legislation is expected in the forthcoming digital services act package, and this will set rules on how companies such as Google, Facebook and Twitter will have to police illegal and possibly harmful content online. Against this background, this paper aims to (1) describe the current EU liability regime for online intermediaries set out under the E-commerce Directive; (2) highlight the implementation gaps that have been identified; and (3) present the main proposals for reforming such an online liability regime and the main policy questions that have been discussed so far.

AUTHOR

Tambiana Madiaga, Members' Research Service, EPRS

This paper has been drawn up by the Members' Research Service, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

To contact the author, please email: eprs@ep.europa.eu

LINGUISTIC VERSIONS

Original: EN

Translations: DE, FR

Manuscript completed in April 2020.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

Brussels © European Union, 2020.

Photo credits: © Maksim Kabakou / Adobe Stock.

PE 649.404
ISBN: 978-92-846-6559-4
DOI:10.2861/08522
QA-04-20-239-EN-N

eprs@ep.europa.eu
<http://www.eprs.ep.parl.union.eu> (intranet)
<http://www.europarl.europa.eu/thinktank> (internet)
<http://epthinktank.eu> (blog)

Executive summary

The E-commerce Directive was adopted in 2000, aimed at harmonising minimum standards of liability for internet (online) intermediaries across the EU. The legislation introduced a 'safe harbour' principle, under which online intermediaries who host or transmit content provided by a third party are exempt from liability unless they are aware of the illegality and are not acting adequately to stop it. They are subject to 'duties of care' and 'notice and take down' obligations to remove illegal online content. Furthermore, under the EU liability regime, online intermediaries cannot be subject to a general obligation to monitor their users' online content – to protect users' fundamental rights such as privacy and freedom of expression – while self-regulation has largely been encouraged for removing and disabling access to illegal information.

However, numerous studies have shown that the way the E-commerce Directive has been implemented across the EU varies greatly and that national jurisprudence on online liability today remains very fragmented, while European Court of Justice case law does not provide sufficient guidance. Several gaps have been identified in this respect. First, it remains unclear to what extent the new type of online services, such as social media companies that have appeared since the adoption of the E-commerce Directive, fall within the definition of 'information society services' providers that can benefit from the liability exemption. Second, the 'safe harbour' conditions and 'notice-and-take down' obligations are unclear essentially because the underlying notions which are used to trigger the liability exemption, such as the distinction between 'passive' role and 'active' and the meaning of 'illegal activities', lack a proper definition. There are also considerable differences both with regard to the definition and the functioning of notice-and-take down throughout the EU. Third, it is becoming difficult to differentiate between prohibited 'general' content monitoring and acceptable 'specific' content monitoring, while automatic filtering mechanisms are increasingly used to detect illegal content.

Against this background, the European Commission is expected to table a proposal to revise the liability regime as part of the forthcoming digital services act. Expert proposals vary from clarifying the current regime of exemption of liabilities to creating a secondary liability regime for online intermediaries. Policy-makers are expected to address a wide range of policy questions. First, an extension of the scope of the EU legislation to encompass both 'illegal' and 'harmful' content has been proposed and the question of whether 'online disinformation' and 'online advertisements' should fall under the scope of the revised liability regime has been raised. Second, setting a robust liability framework relies on defining precise concepts and ensuring compliance with EU fundamental rights, especially with freedom of speech and privacy rights. To that end, academia and stakeholders call for substantial revision of the EU framework, to clarify whether new digital services providers, such as social networks, online advertising services, collaborative economy platforms and online marketplaces, could or could not benefit from the safe harbour regime. This entails a need to clarify the difference between 'active' and 'passive' online intermediaries, to amend and further harmonise the 'notice and take down' regimes, to clarify the use of 'automated filtering' measures and the need for adequate procedural safeguards. Furthermore, the opportunity to enshrine a 'Good Samaritan' clause under EU law, to incentivise online intermediaries to better control the content they host and to include a set of new obligations in the liability regime, as well as to ensure algorithm transparency and neutrality, are discussed. Finally, consideration should be given to the definition of roles and powers granted to digital platform regulators in the EU.

Table of contents

1. E-commerce Directive liability regime: Background	1
1.1. Liability regime: Aim and scope of the directive	1
1.2. Safe harbour regimes and horizontal approach	1
1.3. Duties of care and notice and take down obligations	2
2. Implementation gaps and calls for reform of the E-commerce Directive	4
2.1. Definition of 'information society service' is unclear	4
2.2. Safe harbour conditions and notice and take down obligations are unclear	5
2.3. Duty of care regime and prohibition on general monitoring are unclear	6
3. Revision of the EU liability regime for online intermediaries	7
3.1. Context of the forthcoming digital services act	7
3.2. Proposals for reform: Theoretical framework	8
3.3. Proposals for reform: Policy questions	10
3.3.1. Scope of the liability regime	10
i. Illegal and potentially harmful content	10
ii. Disinformation and 'fake news'	11
iii. Online advertisement	12
iv. Differentiating liability rules for small and large intermediaries	13
3.3.2. Clarifying safe harbour conditions	13
i. Definition of information society service providers	13
ii. Difference between 'active' and 'passive' roles	14
iii. Algorithm transparency and neutrality	14
3.3.3. Revisiting the notice and take down regimes	14
3.3.4. Automated filtering measures and general monitoring	15
3.3.5. Introduction of a 'Good Samaritan' clause	17
3.3.6. Roles and powers of regulators	18
4. Outlook	19
5. References	20

1. E-commerce Directive liability regime: Background

The key principles of the EU liability regime for online intermediaries are enshrined in the E-commerce Directive¹ adopted in 2000. The directive's overarching goal was to foster the development of electronic commerce in the European Union (EU). To that end, the Union set up a common legal framework to ensure the free movement of information society services between Member States and ensure legal certainty and consumer confidence in online commerce. The directive therefore aims at approximating national laws in various fields, including with regard to the establishment of service providers in the EU, rules applicable to commercial communications, electronic contracts and the liability of online intermediaries.²

1.1. Liability regime: Aim and scope of the directive

The E-commerce Directive provisions on liability were adopted to address the divergences observed in court rulings and national legislation that resulted in legal uncertainty for online service providers in the EU and in creating obstacles for the internal market.³ The directive aims therefore at defining a set of specific rules under which 'information society service' providers – commonly referred to as 'online intermediaries' – who host or transmit illegal content provided by a third party are exempt from liabilities when certain conditions are fulfilled. As such, the directive does not provide with a general liability regime for 'online intermediaries' but instead carves out specific rules under which those intermediaries are not held liable under EU law (i.e., safe harbour regimes).

The E-commerce Directive liability rules apply to all 'information society services', defined as services that are 'normally' provided 'for remuneration' by 'electronic means' upon 'an individual request of a user'.⁴ The notion of 'information society services' spans a wide range of online economic activities including selling goods online, offering online information or commercial communications, providing online search tools allowing for search, provision of electronic network and services, video-on-demand or the provision of commercial communications by electronic mail.⁵ As a result, a large array of online actors ranging from traditional electronic communications providers (e.g. internet service providers) to new online intermediaries (e.g. search engines, social media companies, software and game and cloud providers), potentially fall under the scope of the E-commerce Directive.

1.2. Safe harbour regimes and horizontal approach

The E-commerce Directive introduces a safe harbour principle, under which three types of online intermediaries who host or transmit content provided by a third party are exempt from liability under certain conditions.

¹ See [Directive 2000/31/EC](#).

² Only the provisions (i.e. Articles 11 to 15) relating directly to the liability regime will be discussed here. Other issues, including the question of whether or not to maintain the country of origin principle, fall outside the scope of this paper.

³ See European Commission, [EU study on the legal analysis of a single market for the information society: New rules for a new age?](#), 2014.

⁴ See Art. 2(a) of Directive 2000/31/EC (above). See also Article 1 (1) (b) Directive 2015/1535 (which replaced Directive 98/34/EC).

⁵ See Recital 18 of Directive 2000/31/EC (above). Television and radio broadcasting, video-on-demand and the provision of commercial communications by electronic mail are not information society services.

- **Mere conduit service providers** (Art. 12) are exempt from liability when the service provider is only passively involved in the transmission of data (i.e. interconnection to the internet provided by traditional internet service providers and network operators), and,
- **Caching providers** (Art. 13) are exempt from liability when they temporarily and automatically store data in order to make transmission more efficient (e.g. proxy server) and if several technical conditions for storing the information are met (e.g. local copy identical to original), and,
- **Hosting providers** (Art. 14) are exempt from liability when those companies storing data for their users (e.g. webhosting) do not know that they host illegal activity or information and act expeditiously to remove or disable access to the illegal information.

The E-commerce Directive takes a horizontal approach to the liability of 'information society service providers'. That means that, when the conditions are fulfilled, the EU legislation exempts the online intermediaries from a wide array of liabilities including contractual liability, administrative liability, tortious (delictual) or extra-contractual liability, penal liability, civil liability or any other type of liability, for all types of activities initiated by third parties, including copyright and trademark infringements, defamation, misleading advertising, unfair commercial practices, unfair competition, publications of illegal content, etc.⁶ In so doing, a balance between the different interests at stake (e.g. citizens, creators, right holders) must be struck in designing the liability rules.⁷ As a result, the liability rules intend to simultaneously prevent the illegal handling of information on the internet and to ensure the **respect of EU fundamental rights** (e.g. freedom of expression, personal data protection, property rights, freedom to conduct business).

1.3. Duties of care and notice and take down obligations

Under the safe harbour regimes, online intermediaries are immune from liability unless they are aware of the illegality and are not acting adequately to stop it. A conceptual distinction⁸ between online intermediaries' '**passive**' or '**active**' role was developed by the Court of Justice of the European Union (CJEU) on the basis of Recital 42 of the E-commerce Directive, which reads:

The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

According to the CJEU case law in *Google France*⁹ and in *L'Oréal*,¹⁰ the tolerable level of passiveness depends on the intermediaries' roles.

⁶ See European Commission, [EU study on the legal analysis of a single market for the information society: New rules for a new age?](#), 2014.

⁷ Recital 41.

⁸ For an overview, see Institute for Information Law Study for the European Commission, [Hosting Intermediary Services and Illegal Content Online](#), IViR Report for the European Commission, 2018.

⁹ See joined cases, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v Viaticum SA and Luteciel SARL* (C-237/08) and *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* (C-238/08).

¹⁰ See Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others*.

Intermediaries such as 'mere conduit' service providers (Article 12) and 'caching' providers (Article 13) have mostly a passive role and no or limited knowledge about the user content they convey. 'Mere conduit' providers are not liable for the content they convey, as long as they do not initiate the transmission, nor select the receiver or select or modify the information contained in the transmission. 'Caching' providers are also not liable for the automatic, intermediate and temporary storage of information they implement to make information transmission more efficient.

To the contrary, 'hosting providers' (Article 14) play a more active role, with more control over the content they host. They are therefore subject to more stringent 'duties of care' and 'notice and take down' obligations. First, hosting providers are not liable when they do not have 'actual knowledge' of illegal activity or information and are not aware of facts or circumstances from which the illegal activity or information is apparent. What constitutes 'illegal activities' has, however, not been defined precisely in the E-commerce Directive. Second, hosting providers must 'act expeditiously to remove' (i.e. take down) or to 'disable access' (i.e. block) illegal activity or information of which they have obtained actual knowledge. Hosting service providers can benefit from a liability exemption only if those two conditions are fulfilled. Furthermore, the directive does not affect the possibility for Member States to require service providers who host information to apply duties of care under national law to detect and prevent illegal activities. Intermediaries can be subject to injunctive reliefs (i.e. court orders) when they are found to be in breach of specific pieces of legislation (e.g. copyright law).¹¹

Member States **cannot impose a general obligation to monitor** when they implement their duty of care obligation (Article 15). Instead, in order to implement 'duties of care' and 'notice and take down' obligations, the E-commerce Directive asks Member States to encourage voluntary agreements for removing and disabling access to illegal information (Recital 40). Different legal instruments have been set in this regard. **Voluntary codes of conduct** for internet service providers have been adopted in several Member States (e.g. the Netherlands, United Kingdom (UK)). At EU level, the European Commission concluded a Memorandum of Understanding (MoU) on the sale of counterfeit goods on the internet,¹² with major internet platforms and rights holders, to fight intellectual property rights (IPR) infringement. This voluntary agreement aims to prevent offers of counterfeit goods from appearing on online marketplaces. Furthermore, in recent years, the Commission has adopted a number of soft-law instruments encouraging hosting providers to engage in voluntary monitoring, including a Code of Conduct on countering illegal hate speech online,¹³ the 2017 Communication on Tackling Illegal Content¹⁴ and the 2018 Recommendation on Measures to Effectively Tackle Illegal Content Online.¹⁵

¹¹ See OpenForumEurope, [Intermediaries liabilities through the backdoor](#), 2016, at p 6 and 7.

¹² See [Memorandum of Understanding on the sale of counterfeit goods via the internet](#), European Commission, 2016.

¹³ See [The EU Code of conduct on countering illegal hate speech online](#), European Commission, 2016.

¹⁴ See [COM\(2017\) 555 final](#).

¹⁵ See [C\(2018\) 1177 final](#).

2. Implementation gaps and calls for reform of the E-commerce Directive

Various studies and public consultations¹⁶ demonstrate large variances in the way the E-commerce Directive has been implemented throughout the EU and national jurisprudence on liability regimes remain very fragmented. Academics also point to **persisting legal uncertainty** regarding the application of existing national norms and conflicting court rulings between Member States and even within the same jurisdiction.¹⁷ Several implementation gaps have been identified in this respect.

2.1. Definition of 'information society service' is unclear

One of the key questions is to what extent the new type of online services that have appeared since the adoption of the directive fall within the definition of an 'information society service' that is the *sine qua non* condition to benefit from the liability exemption. The case law both at national and European levels shows that **divergences persist among Member States** in many respects.¹⁸

While the E-commerce Directive provides that the liability exemption is applicable to services 'normally provided for remuneration', it is unclear if it applies to 'activities sponsored by advertisements', to 'entirely free models' (e.g. Wikipedia) and to 'freemium models' (i.e. when users make free use of a service and only some of them pay some kind of remuneration).¹⁹ In France, the Paris Court of Appeal ruled in favour of the Wikimedia Foundation,²⁰ defending the Foundation's status as a hosting provider. However, the CJEU found that online publishers of news could be liable for defamatory comments and illegal material published on their website, regardless of whether the content is free or paid for by users, where the platform receives income generated by advertisement.²¹

The national legislation and jurisprudence on liability regimes for hyperlinks and search engines is also very fragmented. A UK court considered hyperlinking to be a mere conduit activity (falling under Art. 12) while a German court considered it to be a form of hosting (falling under Art. 14).²² Spain and Portugal have extended the liability exemption by law to hyperlinking and as well as search engine activities.²³ It is also open to discussion whether the E-commerce liability exemptions apply to blockchain participants,²⁴ while the fact that providers providing cloud computing services

¹⁶ See European Commission, [E-commerce Directive](#), 2020.

¹⁷ See C. Angelopoulos, Beyond the safe harbours: harmonising substantive intermediary liability for copyright infringement in Europe, *Intellectual Property Quarterly*, 2013, 3, 253-274. See also I. Garrote Fernandez-Diez, [Comparative analysis on national approaches to the liability of internet intermediaries for infringement of copyright and related rights](#), 2014.

¹⁸ For an overview, see S. Stalla-Bourdillon, [Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well](#), 2017.

¹⁹ For example, to get more storage capacity.

²⁰ See M. Paulson and J. Rogers, [Victory in France: Court rules in favor of the Wikimedia Foundation](#), Wikimedia Foundation, 2016.

²¹ See [Case 291/13 Pappasavvas](#).

²² See European Commission, [Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce \(2000/31/EC\)](#), 2010.

²³ Ibid.

²⁴ See J. Schroers, [Can blockchain participants use the e-Commerce Directive's liability exemptions?](#), KU Leuven CiTiP, 2019.

(e.g. Google Drive, Apple iCloud, Dropbox) are sometimes considered as hosting providers, has been criticised.²⁵

Furthermore, several academic studies have highlighted the uncertainties surrounding the application of the E-commerce Directive to social media companies and collaborative platforms.²⁶ The CJEU has recently ruled in different ways on the question of whether the service provided by Airbnb and Google must be classified as an 'information society service'. In its 2017 *Uber* case,²⁷ the CJEU decided that Uber does not classify as an 'information society service' subject to the liability rules in the E-commerce Directive but rather as a 'service in the field of transport'. In *Airbnb Ireland*,²⁸ however, the Court held that the services provided by Airbnb Ireland (consisting of connecting, via an online platform, potential guests with hosts offering accommodation to rent) fall within the definition of an 'information society service'. Following the Court's reasoning, the classification as an 'information society service' depended on the degree of control that the platform had over the service provided. The lesser the degree of control, the greater the likelihood of being classified as an information society service. However, some experts stress that the e-commerce harmonisation regime is incomplete as it leaves the question of liability for collaborative economy intermediary activities to be settled under relevant national legislation.²⁹ In addition, CJEU jurisprudence being complex and case specific, there is a risk that national courts will interpret such jurisprudence in different ways, which could result in **legal fragmentation** throughout the EU.³⁰

2.2. Safe harbour conditions and notice and take down obligations are unclear

Under the E-commerce Directive, the hosting company has to act 'expeditiously' to remove or to disable access to the unlawful content upon obtaining 'actual knowledge' of 'illegal content or activities'. However several flaws have been identified.

First, the notions underpinning the safe harbours regime lack clarity. There is no definition of what constitutes 'illegal activities' and no definition of 'actual knowledge'. Depending the implementation path chosen in the Member States, online intermediaries are exempted from liability on different grounds (e.g. if they have knowledge of illegal content, through a court order or a notice, or via general awareness). Furthermore the concepts of 'passive' and 'active' role developed by the CJEU and the reasoning of the Court as regards the requirements of 'control' and 'awareness', lacks clarity.³¹

²⁵ See R. Weber, D. Staiger, [Cloud Computing: A cluster of complex liability issues](#), European Journal of Current Legal Issues, 2014.

²⁶ See [Providers Liability: From the eCommerce Directive to the future](#), Policy Department for economic and scientific policy, Directorate-General for Internal Policies, European Parliament, 2017. See also the study published by the UK Committee on Standards in Public Life, [Intimidation in Public](#), 2017; L. Andrews, [We need European regulation of Facebook and Google](#), London School of Economics blog, 2018; L. Woods, [When is Facebook liable for illegal content under the E-commerce Directive? CGv Facebook in the Northern Ireland courts](#), EU Law Analysis blog, 2017.

²⁷ See [Case C-434/15](#).

²⁸ See [Case C-390/18](#).

²⁹ See Institute for Information Law Study for the European Commission, [Hosting intermediary services and illegal content online](#), 2018, at p 30-31. For an overview of the case law see A. Hoffmann and A. Gasparotti, [Liability for illegal content online: Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act"](#), CEP study, March 2020.

³⁰ See A. Hoffmann and A. Gasparotti, above.

³¹ See S. Stalla-Bourdillon, [Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well](#), 2017.

Second, there are considerable differences both with regard to the definition and the functioning of notice-and-takedown throughout the EU. With regard to the definition of notice and take down mechanisms, Member States have set up different systems including a 'notice and take down' system (i.e. the illegal content must be removed), a 'notice and stay down' system (i.e. the illegal content must be removed and cannot be re-uploaded), or a 'notice and notice system' (i.e. a system in which the hosting provider is only supposed to forward the notification of infringement to the alleged infringer). Some Member States have set no notice and take down mechanisms. This heterogeneity of models across the EU leads to great legal uncertainty for internet intermediaries.³²

With regard to the implementation of notice and take down mechanisms, some Member States require a formal procedure and official notification by judicial authorities, while others only require notification from the right-holder to assume the service provider has 'knowledge' of the illegal content. Also, there is no common understanding of what comprises 'expeditious' action to remove or to disable access to the illegal information. As a result, the timeframe for intervention varies greatly, for instance under the EU Code of Conduct on countering illegal hate speech online, which requires action by the platform in less than 24 hours after being notified, whereas the Dutch notice and take down Code of Conduct mentions the need for such an action within 5 working days following notification, provided the content is not manifestly unlawful or punishable.³³

Furthermore, the **E-commerce Directive does not harmonise the procedural safeguards** and only a few Member States have implemented counter notice procedures enabling the customers to challenge a request to take down allegedly illegal material.³⁴

2.3. Duty of care regime and prohibition on general monitoring are unclear

Article 15 of the E-commerce Directive prohibits Member States from imposing on online intermediaries a general obligation to monitor information that they transmit or store. However, the prohibition refers solely to monitoring of a general nature and does not concern monitoring obligations in a specific case. In fact, in line with national legislation, national courts can impose injunctions on online intermediaries in order to prevent particular infringements (e.g. for instance to enable plaintiffs to enforce their copyright).³⁵ This requires a certain degree of monitoring. However, since the directive does not specify what the duty of care obligations envisaged in national laws to detect and prevent illegal activities entail, the boundary between duties of care and general monitoring is not clear and differentiating 'general' monitoring from 'specific' monitoring obligation is problematic.³⁶

The lack of legal certainty concerning monitoring of online content is reinforced by the fact that large online platforms often have **automated filtering systems**. These measures are implemented based on Recital 40 of the E-commerce Directive, which states that the liability rules do not prevent the development and operation of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology. However, the question as

³² See I. Garrote Fernandez-Diez, above.

³³ See Institute for Information Law Study for the European Commission, above.

³⁴ See European Commission, [EU study on the legal analysis of a single market for the information society: New rules for a new age?](#), 2014.

³⁵ Ibid.

³⁶ See A. Kuczerawy, [To Monitor or Not to Monitor? The Uncertain Future of Article 15 of the E-Commerce Directive](#), KU Leuven CiTiP, 2019.

to whether such proactive measures by online intermediaries to detect and remove illegal content may result in conducting a general monitoring is unlawful under the E-commerce Directive has been discussed (See Box 1 below).

Box 1 – CJEU case law on general monitoring

In *Scarlet v SABAM* (2011)³⁷ and in *SABAM v Netlog* (2012),³⁸ the CJEU ruled that requiring an internet service provider (such as Scarlet, which transmits information over communication networks), or an online social network (such as Netlog, which stores information provided by the users on its servers), to carry out general monitoring and install filtering systems to prevent copyright infringements is illegal pursuant to 15(1) of the E-commerce Directive. However, the judgments do not preclude national judges from imposing narrower filter obligations. In *UPC Telekabel Wien* (2014),³⁹ the CJEU ruled that, based on a court injunction, an internet service provider could block its customers' access to a website that places materials in breach of copyright law.

The CJEU case law requires that a balance is struck between the preventive measures imposed on technical intermediaries and the applicable fundamental rights that would be affected.⁴⁰ National courts must therefore carefully consider fundamental rights and proportionality before any monitoring, filtering or blocking order is made. The companies' freedom to conduct business and the users' right to privacy and the freedom of information must be ensured. However, the CJEU case law is not clear where the balance should lie between the rights of internet users, internet service providers and rights holders.⁴¹

In the recent *Eva Glawischnig-Piesczek v Facebook Ireland* case (2019),⁴² the ECJ was asked to clarify the scope of the obligations that might be imposed on a host provider under the E-commerce Directive. The Court ruled that a social network platform operator, such as Facebook, could be ordered to find and delete comments identical to an illegal defamatory comment, as well as equivalent comments from the same user. According to some experts, this ruling opens the door to obligations being imposed on platforms to proactively monitor content.⁴³ Furthermore, it has been stressed that such an approach would be difficult to implement in practice without also entailing a general monitoring obligation to be performed by the online intermediary.⁴⁴

3. Revision of the EU liability regime for online intermediaries

3.1. Context of the forthcoming digital services act

The European Commission has conducted various assessments of the E-commerce Directive since 2010, with a view to investigating the necessity for its amendment. In a first phase, the European

³⁷ See [Case C-70/10](#).

³⁸ See [Case C-360/10](#).

³⁹ See [Case C-314/12](#).

⁴⁰ See P. Laurent and others, [SABAM v. Netlog \(CJEU C 360/10\) ... as expected!](#), Kluwer Copyright Blog, 2012.

⁴¹ See. C. Angelopoulos, [CJEU in UPC Telekabel Wien: A totally legal court order...to do the impossible](#), Kluwer Copyright Blog, 2014.

⁴² See [Case C-18/18](#).

⁴³ See E. Chelioudakis, [The Glawischnig-Piesczek v Facebook case: Knock, knock. Who's there? Automated filters online](#), KU Leuven CITIP, 2019.

⁴⁴ See E. Rosati, [Material, personal and geographic scope of online intermediaries' removal obligations beyond Glawischnig-Piesczek \(C-18/18\) and defamation](#), *European Intellectual Property Review*, 2019, 41(11), 672-682. See also the case-law before the European Court of Human Rights (ECtHR). The Court delivered its [MTE and Index.hu](#) judgment, concerning the liability of online intermediaries for user comments considered to be hate speech, in 2016.

Commission focused its efforts on developing a **harmonised framework** for EU 'notice-and-action' procedures.⁴⁵ Then, in its 2012 Communication, A coherent framework to build trust in the digital single market for e-commerce and online services,⁴⁶ the Commission acknowledged that despite the guarantees offered by the E-commerce Directive, intermediary internet service providers were facing legal uncertainty given the fragmentation of the applicable rules in the EU. The Commission advocated, however, maintaining the liability regime under the E-Commerce Directive while **encouraging self-regulatory** efforts by platforms.⁴⁷

The **European Parliament** called for clarity on the liability of online intermediaries, given the flaws in enforcement and called for new guidance to enable online platforms to better comply with their responsibilities.⁴⁸ However, instead of launching a revision of the E-commerce Directive, the Commission made the choice to carve out targeted instruments to address specific forms of illegal online content instead. As a result, in recent years, sector-specific legislation has been passed to increase the obligations of online intermediaries to **fight sexual abuse online**,⁴⁹ **copyright infringement** in the context of user generated content uploaded on large platforms⁵⁰ and tackle **hate speech and violence** in the content provided by video-sharing platform providers,⁵¹ while a new regulation on preventing the dissemination of **terrorist content online** is still being discussed.⁵²

Under the new leadership of President von der Leyen, the European Commission finally committed to upgrading the Union's liability and safety rules for digital platforms, services and products, with a new digital services act (DSA).⁵³ The new Commission work programme announced that a draft of the DSA and clearer rules on the transparency, behaviour and accountability of online intermediaries who act as gatekeepers to information and data flows will be released in the fourth quarter of 2020, or early 2021.⁵⁴

3.2. Proposals for reform: Theoretical framework

The E-commerce Directive as it currently stands does not harmonise the conditions for holding intermediaries liable, but instead only the conditions for exempting online intermediaries from liability. Given the gaps identified in section 2 above, academics and experts have discussed extensively how to reform the liability regime. Proposals vary from clarifying the current regime of exemption of liabilities to creating secondary liabilities for online intermediaries. The different scenarios require different types of intervention, ranging from strengthening self-regulation to co-regulation and from a limited harmonisation of substantive law to a more comprehensive harmonisation of substantive law. Some of the most recent proposals are listed below:

⁴⁵ See A. Kuczerawy, [Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative](#), *Computer Law & Security Review*, 2015.

⁴⁶ See [COM\(2011\) 942 final](#).

⁴⁷ The European Commission adopted a [Recommendation on measures to effectively tackle illegal content online](#) (C(2018) 1177 final) and supported the development of the [EU Code of Practice on Disinformation](#) on 1 March 2018.

⁴⁸ See European Parliament [resolution](#) of 15 June 2017 on online platforms and the digital single market, 2016/2276(INI).

⁴⁹ See [Directive 2011/93/EU](#) on combating the sexual abuse and sexual exploitation of children.

⁵⁰ See [Directive 2019/790](#) on copyright and related rights in the digital single market.

⁵¹ See [Directive 2018/1808](#) on the Audiovisual Media Services Directive.

⁵² See [COM\(2018\) 640 final](#). The text has been adopted by Parliament and is now [awaiting](#) its first reading by the Council.

⁵³ See Ursula von der Leyen, [A Union that strives for more – My Agenda for Europe](#), 2019. See also the [mission letter](#) to Margrethe Vestager and [mission letter](#) to Thierry Breton, European Commission, 2019.

⁵⁴ See [Annex 1 of the European Commission work programme](#), 2020.

- Helberg and others⁵⁵ have proposed setting up a framework of **cooperative responsibility for online platforms**. This would require defining the essential public values at play in particular economic and societal activities and develop, through a multi-stakeholder process, commonly agreed regulations, codes of conduct, terms of use and technologies (e.g. 'by design').
- Smet and Angelopoulos⁵⁶ suggest moving away from the traditional horizontal approach of the EU's safe harbour regime, towards a more **vertical approach** to online liabilities, under which distinct actions would be tailored to diverse wrongdoings, e.g. notice-and-notice for copyright, notice-wait-and-takedown for defamation and notice-and-takedown and notice-and-suspension for hate speech.
- Satore⁵⁷ argues that there is a need to introduce **EU rules on secondary liability** (i.e., liability for the illegal activities of their users), covering all kinds of illegal activities that are enabled by the intermediaries. According to his conclusions, the exemption from secondary liability should cover all main intermediaries, including search engines and collaborative platforms as well 'active' intermediaries, as long as their engagement with the activities of their users pertains to their intermediation service. Furthermore, the scope of the duty of care obligation should be specified for different kinds of user activities (e.g. expressive communications between users, the sending of advertisements, economic exchanges, the distribution of malicious software, etc.).
- To the contrary, a study for the European Parliament⁵⁸ suggests there is no pressing need for reform of the E-commerce Directive because its provisions are sufficiently flexible to adopt to new business models, which also make them generally future proof. According to the study prepared for the Parliament, ECJ case law will answer the remaining open legal questions still open, and instead proposes a **sector-specific approach** for setting the liability rules applicable to online intermediaries.
- De Streel, Buiten and Peitz⁵⁹ favour, as a first best option, carving out a **negligence-based system** based on an economic analysis of liability rules. Accordingly, the duty of care of the providers of hosting services could be determined on the basis of a set of general criteria (e.g. instruments available to prevent harm, social costs of precautionary measures, the type and the extent of the harm, the social benefits that the activities of online hosting platforms provide to society, etc.), and differentiated according to the type of illegal material. However, given the political and legal difficulties raised by the harmonisation of national liabilities rules, they instead recommend an approach clarifying hosting providers' liability conditions at EU level. 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.

⁵⁵ See N. Helberg, J. Pierson, and T. Poell, [Governing online platforms: From contested to cooperative responsibility](#), *The Information Society*, 34(1), 2018, p.1-14.

⁵⁶ See C. Angelopoulos and S. Smet, [Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability](#), *Journal of Media Law*, 2016. Going further towards full harmonisation, Angelopoulos also proposed the adoption of a European Civil Code or a European Tort Code replacing national contracts and tort law, which will provide a harmonised legal basis for addressing the internet intermediaries' liability. Nevertheless, this option, requiring a full harmonisation of substantive law, seems unlikely to come about given the fact that it would also raise sensitive issues of subsidiarity and proportionality (see C.J. Angelopoulos, [European intermediary liability in copyright: A tort-based analysis](#), Institute for Information Law, 2016).

⁵⁷ See [Providers Liability: From the eCommerce Directive to the future](#), Policy Department for economic and scientific policy, Directorate-General for Internal Policies, European Parliament, 2017, p.29.

⁵⁸ See [Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?](#), Policy Department for economic and scientific policy, Directorate-General for Internal Policies, European Parliament, 2018.

⁵⁹ See A. de Streel, M. Buiten, M. Peitz, [Liability of Online Hosting Platforms – should exceptionalism end?](#), CERRE, 2018.

3.3. Proposals for reform: Policy questions

Independently of the chosen approach, EU policy-makers will have to address a range of questions, some of which are listed below:⁶⁰

3.3.1. Scope of the liability regime

One of the fundamental questions policy-makers are facing is how to define the scope of a revised liability regime. Several issues would need to be considered, in particular, the opportunity to address both 'illegal' and 'harmful' content, dis- and misinformation ('fake news') and online advertisements under the revised liability regime for online intermediaries.⁶¹

i. Illegal and potentially harmful content

The current liability regime addresses only 'illegal content', but as highlighted above, the E-commerce Directive does not provide a precise definition of this notion. 'Illegal content' arguably encompasses a large variety of content categories that are not compliant with EU and national legislation, including on online violations of copyright, trademark and trade secrets; counterfeiting and unauthorised parallel distribution via the internet; on consumer protection violations, privacy, libel and defamation law violations; data protection violations; hate speech and incitement to violence (e.g. terrorism content); and child sexual abuse material and disclosure of private sexual images without consent ('revenge porn').⁶²

In contrast, potentially 'harmful content' refers to content which often does not strictly fall under the prohibition of a law, but might nevertheless have harmful effects. A wide range of content potentially falls into this category including harassment arising from social media and messaging services such as bullying, publication of information covered by freedom of speech but which could have a detrimental impact and disinformation content, mis- or disinformation ('fake news') that may hamper the ability of citizens to take informed decisions.⁶³

Harmful content (which is not illegal) does not fall under the E-commerce Directive liability regime so far. However, the EU has recently adopted a range of self-regulatory measures to better control online platform behaviour, in particular the disinformation phenomenon prompted by the use of social media (see below). Furthermore, the EU has attempted to address specific harmful content by way of targeted legislation such as the proposed regulation on preventing the dissemination of terrorist content online that is being discussed by EU legislators that carves out a mandatory duty of care obligation for all platforms to ensure they are not misused for online dissemination of terrorist content.⁶⁴

In the context of the reform of the E-commerce Directive, some academics stress that the current policy approach in the European Union should shift from intermediary liability to intermediary responsibility and support a liability regime for online intermediaries addressing both 'illegal' and

⁶⁰ In addition, the interplay of the liability regimes with other EU rules will need to be considered, including consumer protection, data protection and competition rules.

⁶¹ Other issues will need to be addressed. For an in-depths analysis see A. Hoffmann and A. Gasparotti, above. They call in particular for assessment of the need to extend the scope of the liability rules to service providers established in a third country.

⁶² See Institute for Information Law Study for the European Commission, above.

⁶³ See A. Hoffmann and A. Gasparotti, above. See the proposed taxonomy by L. Woods and W. Perrin, [Online harm reduction – a statutory duty of care and regulator](#), Carnegie Trust UK, 2019.

⁶⁴ The [text](#) has been adopted by Parliament and is now awaiting its first reading by the Council.

'harmful' content.⁶⁵ In this way, some national law-makers are considering differentiating what action is expected from online providers in response to illegal content and activity from action expected from them to tackle potentially harmful conduct that may not be illegal, such as online bullying or intimidation in public life.⁶⁶ Such an approach is also favoured by large online platforms, who have called for the adoption of a two-fold EU framework that would clearly distinguish between the principles of responsibility and liability.⁶⁷

However, a difficult point is that this approach requires **distinguishing what is 'illegal content' online from content which is 'harmful'** but not illegal, while the concept of 'harmful' is subjective, depends greatly on context and can vary considerably between Member States.⁶⁸ Furthermore, fundamental rights defenders argue that introducing rules to address online harmful content into EU law would have grave consequences for freedom of expression, freedom to seek information, and other fundamental rights and therefore seek to strictly limit the scope of the digital services act to illegal content.⁶⁹ Setting a robust framework and ensuring legal certainty will rest on defining precise concepts that comply with EU fundamental rights principles.

ii. Disinformation and 'fake news'

The EU has so far supported a self-regulatory approach to fight the disinformation phenomenon and the spread of 'fake news' online. The European Commission supported the development of the **EU Code of Practice on disinformation** which has been signed voluntarily by leading platforms such as Facebook, Google, Microsoft, Mozilla or Twitter, which submitted to transparent self-regulation.⁷⁰ However, despite their efforts, the ability of the online platforms to contain the spread of misleading information, for instance in the context of the coronavirus pandemic, has been questioned. As a result, some are calling to reassess the current self-regulatory framework.⁷¹

In addition, at national level, several Member States have already designed specific **national legislation** to strengthen compliance rules for social network providers.⁷² In Germany,⁷³ the 2017 law on improving law enforcement in social networks imposes that social networks such as Facebook or Twitter fight unlawful content including hate crime or false messages posted on social network platforms and that they block access to 'manifestly unlawful' content, as well as content that is 'not obviously illegal'. In France,⁷⁴ a law on 'fake news'⁷⁵ was passed in 2017 and a draft law is under discussion on blocking access to content within 24 hours of receipt of a complaint regarding

⁶⁵ See L. Woods and W. Perrin, above. In the same way, see also J. Bayer, [Between Anarchy and Censorship Public discourse and the duties of social media](#), May 2019.

⁶⁶ See [UK Online Harms White Paper - Initial consultation response](#), February 2020.

⁶⁷ See EDiMA, [Responsibility Online](#), 2020.

⁶⁸ See EDRI, [More responsibility to online platforms – but at what cost?](#), 19 July 2019.

⁶⁹ Ibid. EDRI states: 'While the definition of what is illegal is decided as part of the democratic process in our societies, it is unclear which content should be considered "harmful" and who makes that call. Moreover, the term "harmful" lacks a legal definition, is vague and its meaning often varies depending on the context, time, and people involved. The term should therefore not form the basis for lawful restrictions on freedom of expression under European human rights law.'

⁷⁰ See [EU Code of Practice on Disinformation](#), European Commission, June 2019.

⁷¹ See E. Shattock, [Is it time for Europe to reassess internet intermediary liability in light of coronavirus misinformation?](#), European Law Blog, April 2020. The Instagram social network changed its policy in order to provide its users with credible information on the coronavirus pandemic and expand its efforts to remove potentially harmful misinformation. Nevertheless numerous false and misleading stories have thrived on digital platforms.

⁷² For an overview see A. Hoffmann and A. Gasparotti above.

⁷³ See Bundesministerium der Justiz und für Verbraucherschutz, [Netzwerkdurchsetzungsgesetz](#), April 2020.

⁷⁴ See Assemblée Nationale, [Proposition de loi visant à lutter contre les contenus haineux sur internet](#), January 2020.

⁷⁵ See [LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information](#).

content reported as 'patently illegal'. This trend creates a risk of legal fragmentation, while online platforms are de facto providing services on an EU-wide scale.

Against this background, some experts support amendment of the current EU liability regime. One proposal is to define a separate category of service providers in the E-commerce Directive that should not be liable for third-party content and not be obliged to monitor third-party content – since they cannot decide on the legal or illegal quality of content – but should be responsible for administering their platforms in full respect of a set of specific obligations (e.g. maintain ideologically neutral services, create algorithms fostering and promoting diversity of content, ensure transparency of their algorithms and offer options to users in selecting their settings for content, including diversity and the option to identify and disable fake accounts).⁷⁶ In the same way, platform providers could be granted immunity for content in a similar way as for hosting providers and be made responsible for the activities that they actually perform, such as facilitation, dissemination or profiling.⁷⁷ Taking account of the changing audiovisual and media ecosystem, some stakeholders strongly support the enactment of new online liability rules proposed under the forthcoming digital services act, for tackling the online disinformation phenomenon properly.⁷⁸

However, the adequacy and effectiveness of imposing hard law content moderation to control disinformation has been met with scepticism. It has been stressed that setting such EU legislation to protect freedom of expression may be premature and potentially detrimental with regard to fundamental rights.⁷⁹ Concerns have been expressed that command and control regulation would not achieve meaningful results in the field of 'fake news' and that imposing rigid solutions could amount to **censorship**.⁸⁰

iii. Online advertisement

The related question of whether the **spreading of false or misleading online advertisements** should fall in the scope of the revised liability regime has also been raised. The possibility to hold platforms liable for abuses of social endorsement mechanisms and require them to take down infringing content could be considered.⁸¹ Other intrusive measures such as requiring platform providers to identify advertisers and enable users to access this information and maintain a searchable repository of political and issue-based advertising targeting persons in the EU has been proposed.⁸² Against this background, some policy-makers have called for a revision of EU legislation in order to mandate platforms to actively monitor the advertisements shown on their sites and to establish a different set of rules for advertisements for commercial products and services and advertisements of a political nature.⁸³ Furthermore, the necessity of requiring online platforms to

⁷⁶ See [Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States](#), Policy Department for Citizens' Rights and Constitutional Affairs, Directorate General for Internal Policies of the Union, European Parliament, 2019.

⁷⁷ See J. Bayer, [Between Anarchy and Censorship Public discourse and the duties of social media](#), CEPS, May 2019.

⁷⁸ For instance, see [Association of Commercial Television in Europe press release](#), 16 April 2020.

⁷⁹ See STOA, [Regulating disinformation with artificial intelligence](#), European Parliamentary Research Service, European Parliament, 2019.

⁸⁰ See [The legal framework to address "fake news": possible policy actions at the EU level](#), Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, European Parliament, 2018.

⁸¹ See European Commission, [Behavioural Study on Advertising and Marketing Practices in Online Social Media](#), 2018.

⁸² See Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States,, above.

⁸³ See [Draft Opinion of the Committee on the Internal Market and Consumer Protection](#) for the Committee on Legal Affairs with recommendations to the Commission on Digital services act: adapting commercial and civil law rules for commercial

put effective and appropriate safeguards in place to tackle the appearance of advertisements for unsafe products could be further investigated.⁸⁴

iv. Differentiating liability rules for small and large intermediaries

The current liability rules apply to all information society services regardless of their market status or market power. The possibility to define a set of supplementary obligations imposed on large intermediaries, given their large or significant market status, has been identified.⁸⁵ The Copyright Directive gives an example of such differentiation of obligations, as it imposes stringent obligations on online service providers whose main purpose is to store and provide public access to a 'large amount of copyright-protected works'. However, such an approach has been criticised because the notion of 'large amount' creates considerable uncertainty, leaving it to the courts to define its scope.⁸⁶ In addition, any adverse changes to the liability regime – such as increased legal obligations on online intermediaries – could have a handicapping effect on innovation and the activity of online intermediaries.⁸⁷ The guiding factors in differentiating obligations for small and large intermediaries would therefore need to be based on precise legal concepts and their economic impacts properly assessed.

3.3.2. Clarifying safe harbour conditions

Experts and stakeholders call for revision of the E-commerce Directive primarily to clarify several legal notions which underpin the safe harbour regime and in particular the definition of 'information society service providers' and the difference between 'active' role and 'passive' role. Furthermore, the possibility of imposing algorithm transparency and neutrality in order to grant liability/responsibility immunity for online intermediaries should be assessed.

i. Definition of information society service providers

Because the liability regime potentially applies to a much larger variety of services than was the case at the time of its adoption in 2000, the definition of 'information society service providers' would need to be amended to cover new categories of providers whose liability could be triggered.⁸⁸ A revised definition could clarify whether **new digital services providers** (such as cloud infrastructures, content distribution network, search engines, social networks and media-sharing platforms, online advertising services, digital services built on electronic contracts and distributed ledgers such as blockchain), or **collaborative economy platforms** (such as AirBnB and Uber) and **online marketplaces** (used to provided legal but also illegal and counterfeit products), could or could not benefit from a safe harbour regime.

entities operating online (2020/2019(INL)), Committee on the Internal Market and Consumer Protection, European Parliament, 2020.

⁸⁴ See [Draft report on addressing product safety in the single market \(2019/2190\(INI\)\)](#), Committee on the Internal Market and Consumer Protection, European Parliament, April 2020.

⁸⁵ See A. Hoffmann and A. Gasparotti above. See also the recent [draft opinion](#) of the European Parliament Committee on the Internal Market and Consumer Protection on the digital services act and fundamental rights issues posed (2020/2022(INI)). The text stresses that 'SMEs and large players have differing capabilities with regard to the moderation of content; warns that overburdening businesses with disproportionate new obligations could further hinder the growth of SMEs and require recourse to automatic filtering tools, which may often lead to the removal of legal content'.

⁸⁶ See T. Spoerri, [On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market](#), *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2019.

⁸⁷ See Copenhagen Economics, [Online Intermediaries: Impact on the EU economy](#), EDiMA, 2015.

⁸⁸ See C. Del Federico, [Intermediary liability. The "Achilles' heel" of the current legislation: the courts. A comparative analysis with the US, focusing on copyright infringement](#), 2015.

ii. Difference between 'active' and 'passive' roles

The difference between 'active' role and 'passive' role could be clarified for a range of new activities including distribution and processing of third-party data, networking (i.e. connecting users), collaboration (i.e. allowing multiple users to access and edit stored data), matchmaking (i.e. linking supply and demand), indexation (i.e. searchable index) and ranking services (i.e. ranking mechanisms) under the EU liability regime.⁸⁹ Some experts stress that the differentiation of the active/passive role is questionable and complicated for collaborative economy services (such as AirBnB, Uber). They propose alternatively using more appropriate concepts, building on notions such as whether the providers have 'editorial functions', 'actual knowledge' and a 'certain degree of control', which would be more precisely delimited under EU legislation and case law.⁹⁰

Also a shift from today's merely ex-post control (i.e. imposition of injunction reliefs only once detection of illegal conduct has been established) to a more stringent ex-ante control (i.e. ex-ante monitoring of online content) to better control the digital platforms increasingly acting as **'digital gatekeepers'** could be considered.⁹¹ The choice between ex-ante and ex-post control will be particularly relevant for framing the policy discussion on algorithm transparency and neutrality.

iii. Algorithm transparency and neutrality

The possibility of imposing a new set of obligations to grant liability/responsibility immunity to online intermediaries over misinformation and/or online advertisements has been discussed (see above). Should the EU legislator choose this path, the question of ensuring algorithm transparency and neutrality will become central.

It has been proposed, inter alia, to oblige platforms to ensure their algorithms do not systematically favour any political, ideological or religious opinion, or give preference to content that is their own or produced by an affiliated company. Furthermore, following the model of the algorithm transparency requirements imposed by the recent regulation on online platform-to-business relationships,⁹² online users could be offered more control, such as the possibility to prioritise content that is found to be trustworthy by independent news organisations.⁹³

3.3.3. Revisiting the notice and take down regimes

Several proposals have been made to amend the notice and take down regimes implemented in the EU today. Different notice and take down regimes could be set depending on the type of liability at stake, i.e. breach of criminal law (e.g. child sexual abuse) and civil law (e.g. copyright).⁹⁴ An alternative proposal is to move from the horizontal approach of the EU's safe harbour regime, towards a more vertical approach with a calibrated system of notice and action, aiming to achieve viable compromises between conflicting fundamental rights in cases of intermediary liability. Distinct 'actions' tailored to diverse wrongdoings, e.g. notice and notice for copyright, notice wait

⁸⁹ See Institute for Information Law Study for the European Commission, above.

⁹⁰ See A. Hoffmann and A. Gasparotti, above.

⁹¹ For an overview on this line of thinking see P. Alexiadis and A. de Streel, [Designing an EU Intervention Standard for Digital Platforms](#), EUI Working Papers, RSCAS 2020/14. See also E. Laidlaw, [Internet Gatekeepers, Human Rights and Corporate Social Responsibilities](#), London School of Economics, 2012. For some first proposals in this area see European Parliament, [Report of the Committee on the Internal Market and Consumer Protection on the Digital Services Act](#), (2020/2018(INL)), April 2020.

⁹² See [Regulation \(EU\) 2019/1150](#) on promoting fairness and transparency for business users of online intermediation services.

⁹³ See J. Bayer and others above.

⁹⁴ See EDRI [response](#) to the Consultation on Clean and Open Internet, 2015.

and take down for defamation and notice and take down and notice and suspension for hate speech.⁹⁵

However, a pure **self-regulation approach has been very much criticised**. The voluntary codes of conduct developed by online intermediaries, either ex-post (i.e. content removal, account termination or personal data disclosure procedures), or ex-ante (i.e. content filtering), raise serious human rights objections and suffer from a 'democratic deficit' since consumer and citizen involvement is limited.⁹⁶ The adoption of a more detailed notice and take down regime – based on the model of the Digital Millennium Copyright Act in the United States of America (USA) – which describes in detail the legal effect of triggering the notice and take down regime and includes procedural rules, could be a more appropriate approach.⁹⁷ Furthermore, it has been stressed that setting up a detailed and harmonised European notice and take down procedure would provide more legal certainty.⁹⁸

3.3.4. Automated filtering measures and general monitoring

The prohibition of a general monitoring obligation under the E-commerce Directive is regarded by most academics and commentators as a cornerstone of the EU online liability regime that must be maintained.⁹⁹ However, while the current policy thinking in the EU is shifting from implementing intermediary liability to fostering intermediary responsibility, the principle prohibiting general monitoring is de facto being challenged¹⁰⁰ by the use of automated filtering technologies.¹⁰¹

Content recognition tools such as Rights Manager (Facebook) and Content ID (YouTube) already play a major role in copyright protection (See Box 2).¹⁰² Such automated measures have been enshrined or proposed in several pieces of legislation. Article 17 of the 2019 EU Copyright Directive places great emphasis on the adoption of such automatic filtering systems and such large platform automatic filters will likely become the new industry standard.¹⁰³ The proposed regulation on terrorist content also specified that hosting service providers must, where appropriate, take proactive measures to protect their services against the dissemination of terrorist content, including by deploying automated detection tools.¹⁰⁴

⁹⁵ See C. Angelopoulos and S. Smet, above.

⁹⁶ See B. Hugenoltz, [Codes of Conduct and Copyright Enforcement in Cyberspace](#), in Copyright Enforcement and the Internet (ed. Stamatoudi), Kluwer Law International, 2010.

⁹⁷ See Ibid.

⁹⁸ See report from OpenForumEurope, [Intermediaries liabilities through the backdoor](#), 2016. See also C. Del Federico above. See as well the [draft report](#) from the European Parliament Committee on Legal Affairs with recommendations to the Commission on a Digital Services Act, 2020/2019(INL). The draft report proposes to set a harmonised standard procedure for content moderation to follow throughout the Union.

⁹⁹ See A. de Streel, M. Buiten, M. Peitz, above.

¹⁰⁰ See A. Kuczerawy, [To Monitor or Not to Monitor? The Uncertain Future of Article 15 of the E-Commerce Directive](#), KU Leuven CiTiP, 2019.

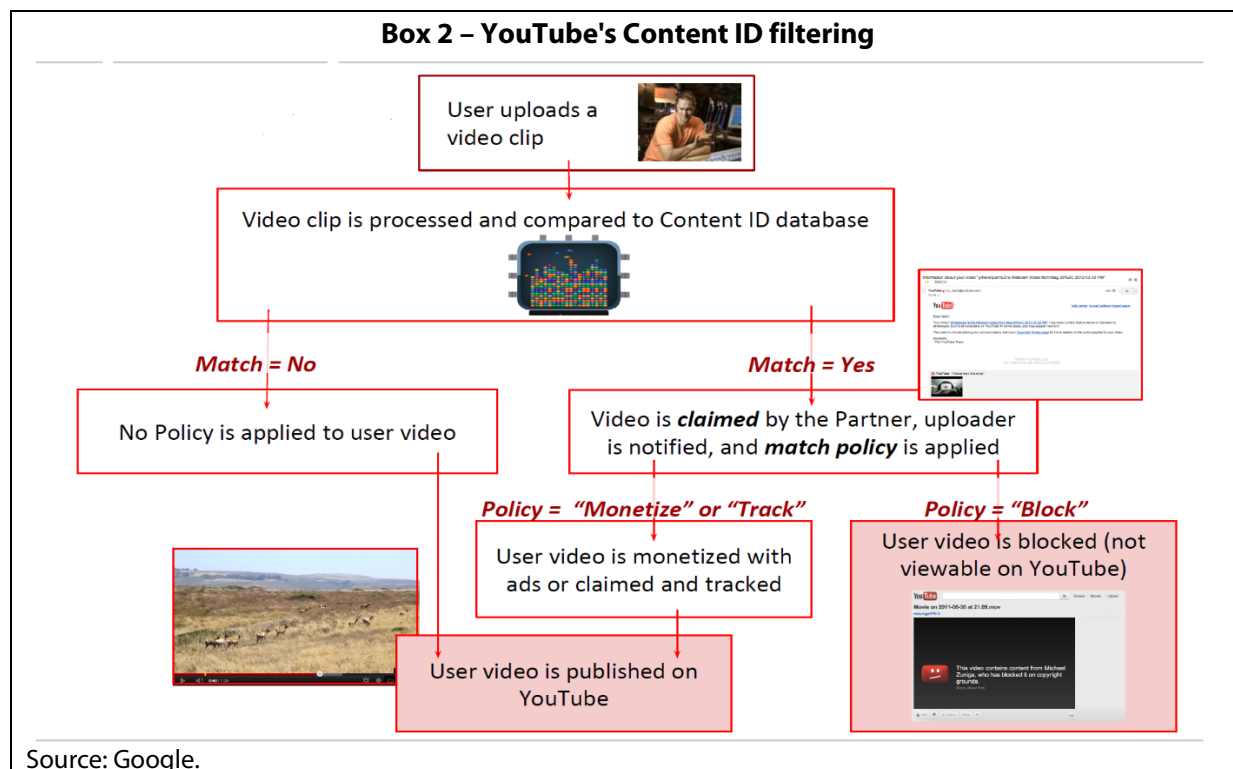
¹⁰¹ Internet filters are content-control software that restrict or control the content an internet user can access, and determine what content will be available or be blocked. The filters' function is to recognise certain content, and then automatically delete it if required.

¹⁰² See French High Council for Literary and artistic property, [Report by the research mission on recognition tools for copyright-protected content on digital platforms](#), JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, 2016. Google is reporting that 98 % of its copyright disputes are processed using Content ID, while only 2 % use the notice and take down procedure.

¹⁰³ See T. Spoerri, [On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market](#), JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, 2019.

¹⁰⁴ See [Article 6\(1\)](#).

Against, this background, the question of mandating that online intermediaries use automated filtering technologies to establish illegal or harmful content will likely become a focus of the discussion on the revision of the E-commerce Directive.



However, such measures present significant drawbacks, including a lack of transparency concerning how the technologies work, a lack of adequate procedural safeguards and a risk of over-enforcement, with online providers being more likely to apply an algorithm that takes down too much, rather than too little, content.¹⁰⁵ Opponents stress above all that filtering algorithms make too many mistakes (i.e., false-positives), because they do not understand context, political activism, or satire, and require human review to prevent fundamental rights violations and discrimination.¹⁰⁶

Furthermore, experts warn that provision fostering the use of upload filters such as that enshrined in the Copyright Directive may indirectly result in general monitoring unless appropriate safeguards are provided.¹⁰⁷ A pending ECJ case may provide some guidance in this respect (see Box 3 below). However, for greater legal certainty, the digital services act could also define precisely when the use of the automated measures should be imposed as a legal obligation for platforms, as well as the associated procedural safeguards and options for judicial redress.¹⁰⁸

¹⁰⁵ See T. Riis and S. Schwemer, [Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation](#), *Journal of Internet Law*, Vol. 22, No 7, 2019, p. 1–21.

¹⁰⁶ See T. Spoerri, [On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market](#), *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2019. See also EDRI, [More responsibility to online platforms – but at what cost?](#), July 2019.

¹⁰⁷ See J. Quintais, [The New Copyright Directive: A tour d'horizon – Part II \(of press publishers, upload filters and the real value gap\)](#), Kluwer Copyright Blog, 2019. See J. Quintais and others, [Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics](#), Institute for Information Law, 2019.

¹⁰⁸ See, for instance, Access Now, [26 recommendations on content governance](#), 2020. This organisation, which defends the digital rights of users, stresses that the use of automated measures should be accepted only in limited cases of manifestly illegal content that is not context-dependant (e.g. sexual abuse against minors).

Box 3 – Filtering systems and Article 11 of the Charter of Fundamental Rights of the European Union

Article 11 (*Freedom of expression and information*) of the Charter of Fundamental Rights of the European Union¹⁰⁹ provides that 'everyone has the right to freedom of expression', including 'freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers' and that 'the freedom and pluralism of the media shall be respected'.

According to the European Court of Justice (ECJ) *Scarlet Extended*¹¹⁰ and *Netlog*¹¹¹ judgments, an order to implement filtering systems that remove legal content may violate the freedom of information pursuant to Article 11 of the EU Charter.

In a pending case, Poland is challenging the legality of Article 17 of the Copyright Directive in the ECJ, on the grounds that the provisions imposing upload filters are contrary to Article 11 of the Charter of Fundamental Rights of the European Union, as they de facto impose upon intermediaries that they automatically filter user uploads on their platforms.¹¹²

3.3.5. Introduction of a 'Good Samaritan' clause

The '**Good Samaritan paradox**' refers to the fact that a hosting intermediary would be disincentivised from taking precautions against infringement for fear of losing safe harbour protection.¹¹³ In other words, the prohibition on playing an active role as a hosting provider may lead hosting providers to avoid making all necessary efforts to assess whether the content they host is illegal in order precisely to avoid being considered as playing an active role.

There is controversy as to whether or not the E-Commerce Directive does contain a 'Good Samaritan' clause – based on the model of the USA Communications Decency Act¹¹⁴ – that protects online providers from civil liability in case voluntary screening or blocking measures are not efficient in completely restricting access to or availability of offensive content. In its 2017 Communication on tackling illegal content,¹¹⁵ the European Commission stresses that hosting providers falling under Article 14 of the E-commerce Directive will not be punished if they take proactive steps to detect, remove or disable access to illegal content (i.e. 'Good Samaritan' actions). However, it has been stressed that the European Commission interpretation is somewhat confusing and misleading because online intermediaries in the EU cannot benefit from the liability exemption if they fail to remove the illegal content at stake.¹¹⁶ In the same way, a 2018 study stresses that, in the absence of a 'Good Samaritan' defence, hosting intermediaries are exposed to a higher risk of liability if they decide to be more active in addressing illegal content proactively.¹¹⁷

To remedy this shortcoming, there are calls to explicitly include a 'good Samaritan' clause in the EU legislative framework. A specific provision could make clear that measures taken in line with Article

¹⁰⁹ [Charter of Fundamental Rights of the European Union](#), 2000/C 364/01.

¹¹⁰ [Case C-70/10](#).

¹¹¹ [C-360/10](#).

¹¹² See [Case C-401/19](#).

¹¹³ See P van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach', *Common Market Law Review*, 2011.

¹¹⁴ See United States Congress, [Communications Decency Act of 1995](#).

¹¹⁵ See [COM\(2017\) 555 final](#).

¹¹⁶ See A. Kuczerawy, [The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?](#), KU Leuven CiTiP, 2018.

¹¹⁷ See Institute for Information Law Study for the European Commission, above.

13(1) should not deprive the intermediary from safe harbour protection.¹¹⁸ Introducing such a clause in EU law could reassure intermediaries that they will not be held liable for hosting illegal material of which they obtained knowledge through their voluntary, proactive monitoring efforts and may also avoid underinvestment by online intermediaries in setting proper mechanisms to find illegal material.¹¹⁹ Internet providers and large platforms support the adoption of a 'Good Samaritan clause' that extends protection from liability in cases where internet intermediaries have actual knowledge of allegedly illicit content when they apply in good faith procedures designed to tackle such content.¹²⁰

However, critics stress that such an amendment to Article 14 of the E-commerce Directive does not seem to be justified, since the case law shows that the courts do not hold platforms using Good Samaritan mechanisms to be liable.¹²¹ For instance, courts have not considered that the use of YouTube's Content ID led to YouTube playing an active role in the provision of its users' content. Such 'Good Samaritan' protection also presents some disadvantages, including the fact that it could encourage excessive take downs on the intermediary's own initiative.¹²²

3.3.6. Roles and powers of regulators

The need to ensure appropriate **regulatory oversight** of online intermediaries in the EU has been raised. Addressing the enforcement issues and institutional design are however uncharted territory, since the E-commerce Directive does not touch upon those issues. Harmonisation, or at the very least, approximation of national institutional and procedural rules would be useful to set up a more efficient common liability online regime applicable across the EU.

The creation of new structures for regulating digital platforms (i.e. central regulator, decentralised system, extension of the powers of existing regulatory authorities) and the definition of roles and powers granted to digital platform regulators (e.g. powers to require additional information, complaint handling, power to impose fines or other corrective action, approval of codes of conduct), could be assessed in the context of the digital services act.¹²³ Setting up an EU regulatory body leading the supervision has been proposed, to ensure oversight and enforcement of the new rules, in particular in complex cross-border situations where it is difficult to implement and enforce rules in an effective manner.¹²⁴

¹¹⁸ See C. Angelopoulos, [Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market](#), 2017.

¹¹⁹ See A. de Streel, M. Buiten, M. Peitz, above. See also Institute for Information Law Study for the European Commission, above.

¹²⁰ See [EuroISPA Consensus Position: Principles for the Future of the EU Intermediary Liability Framework](#), June 2019.

¹²¹ See [Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?](#), Policy Department for economic and scientific policy, Directorate-General for Internal Policies, European Parliament, 2018.

¹²² See A. Kuczerawy, [The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?](#), KU Leuven CiTiP, 2018.

¹²³ See A. Hoffmann and A. Gasparotti above.

¹²⁴ Ibid. See also European Parliament, [Report of the Committee on the Internal Market and Consumer Protection on the Digital Services Act](#), (2020/2018(INL)), 2020.

4. Outlook

There are strong arguments today for reforming the EU liability regime for online intermediaries. Several implementation gaps have been identified. Persisting legal uncertainty regarding the application of existing norms and conflicting court rulings have been highlighted. Technologies and business models have evolved in the last 20 years and the EU framework struggles to capture liability issues raised by new actors such as search engines, social networks or online marketplaces, while the European Court of Justice case law does not provide sufficient guidance. Furthermore, societal challenges have changed the nature and scale of the issue, with the development of a range of new harmful online practices such as the dissemination of terrorist content online, the increasing use of platforms to distribute counterfeit products and the spreading of false or misleading news and online advertisements. Against this background, there seems to be considerable support from academics, stakeholders and policy-makers for reform of the current EU liability regime. However, there is also strong disagreement on the way forward and on how to adapt the EU rules to the new digital environment. Different types of policy intervention, including strengthening self-regulation, fostering co-regulation and promoting a limited harmonisation of substantive law or a more comprehensive harmonisation of substantive law, will need to be addressed in the discussions of the forthcoming digital services act. A question which seems central to the debate is whether it is necessary to extend the scope of the EU legislation to encompass both 'illegal' and 'harmful' content – arguably including even 'online disinformation' and 'online advertisement'. The potential benefits of the policy intervention must be weighed against the risks for fundamental rights.

5. References

- Angelopoulos C. and Smet S., [Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability](#), *Journal of Media Law*, 2016.
- Bayer J., [Between Anarchy and Censorship Public discourse and the duties of social media](#), May 2019.
- De Streel A., Buiten M., Peitz M., [Liability of Online Hosting Platforms – should exceptionalism end?](#), CERRE, 2018.
- European Parliament, [Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States](#) Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies of the Union, European Parliament, February 2019.
- European Parliament, [Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?](#), Policy Department for economic and scientific policy, Directorate-General for Internal Policies, European Parliament, 2018.
- European Parliament, [Providers Liability: From the eCommerce Directive to the future](#), Policy Department for economic and scientific policy, Directorate-General for Internal Policies, European Parliament, 2017.
- Helberg N., Pierson J., and Poell T., [Governing online platforms: From contested to cooperative responsibility](#), *The Information Society*, 2018.
- Hoffmann A. and Gasparotti A., [Liability for illegal content online Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a 'Digital Services Act'](#), CEP, 2020.
- Institute for Information Law Study for the European Commission, [Hosting Intermediary Services and Illegal Content Online](#), 2018.
- Kuczerawy A., [Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative](#), *Computer Law & Security Review*, 2015.
- Riis T. and Schwemer S., [Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation](#), 2019.
- Stalla-Bourdillon S., [Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well](#), in Taddeo M., Floridi L. (eds), *The Responsibilities of Online Service Providers. Law, Governance and Technology Series*, vol 31. Springer, Cham, 2017.
- Woods L. and Perrin W., [Online harm reduction – a statutory duty of care and regulator](#), 2019.

The European Union is expected to revise the liability regime for online intermediaries in the forthcoming digital services act. This publication describes the current liability regime set out under the 2000 E-commerce Directive, highlights the implementation gaps that have been identified, and presents the main proposals for reform that have been discussed so far. Technology has evolved in the last 20 years and new societal challenges, such as the increasing use of platforms to access and distribute products, services and information have arisen. As a result, policy-makers will have to address a range of questions, including the extension of the scope of the liability regime and the revision of the liability exemption conditions.

This is a publication of the Members' Research Service
EPRS | European Parliamentary Research Service

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.



PE 649.404
ISBN 978-92-846-6559-4
doi:10.2861/08522