3. Detailed Analysis of the E-Commerce Directive

After the overview of relevant legislative acts and non-binding policy documents of relevance for online content dissemination, the following chapter takes a detailed look at the provisions of the ECD[413] and their interpretation by the CJEU.

3.1. Scope of Application

3.1.1. Territorial Scope

There are no explicit or specifically laid down rules on territorial scope in the ECD. Recital 58 specifically excludes any extraterritorial scope of this Directive. This means that content originating from information society service providers outside the EU that target EU customers does not fall within the scope of that Directive. Member States are therefore at liberty to take action according to their national law concerning content supplied from providers based outside the EU. However, the Directive reminds of the necessity to consider existing international rules, especially where discussions about the area covered by the Directive have been led in international organisations such as the World Trade Organization (WTO) and the Organisation for Economic Co-operation and Development (OECD).[414] The Recitals point out that any diverging rule could undermine the EU's negotiating position in such international fora.[415] This implies that Member States' action should not contrast with the non-discrimination principles laid down for example in WTO rules, such as most-favoured-nation or national-treatment principles.

The ECD is therefore solely concerned with regulating the activities of information society service providers within the single market. From the perspective of the legislative bodies of the EU, the country-of-origin principle constituted the best regulatory choice to protect internal market princi-

413 The provisions of the ECD relevant in the context of this study are reprinted in the Online Annex, available at www.nomos-shop.de/44382, II. A.
414 Recital 58 ECD.
415 Recital 59 ECD.

ples for the emerging Internet service sector at the time and to protect, by setting some principles and standards, against the threats of legislative forum shopping[416] and a fragmentation of rules[417].

This contrasts with other more recently passed EU acts and legislative proposals that deal with matters of the information society and digital content. The General Data Protection Regulation[418] and the proposed Regulation to prevent the dissemination of terrorist content online[419] extend to information society service providers from third countries that target EU residents. The AVMSD applies to VSP providers from third countries with a market attachment to the EU which can follow from a subsidiary or parent of the service provider established in the EU.[420]

3.1.2. Functional Scope

The functional scope of the ECD is set by the coordinated field of activities. According to Art. 2 lit. h ECD, the coordinated field consists of all legal requirements set by Member States that apply to information society service providers or information society services, without regard as to whether they are general or specific measures. More specifically, the coordinated field covers therefore requirements that are necessary for the taking-up and the pursuit of activities by a service provider. These are requirements relating to authorisation and qualifications, the behaviour of the service provider, the quality of content, provisions relating to advertisement, contracts and the liability of intermediary service providers. Art. 2 lit. h point (ii) provides important exemptions to the coordinated field, namely requirements that are applicable to goods as such, their delivery and to services which are not provided by electronic means. The meaning of this provision is further explained in Recital 21.

The scope of the coordinated field should be strictly limited to the online activities of service providers, such as online information, online ad-

416 Recital 57 ECD.
417 Recital 59 ECD.
418 Art. 3 para. 2 GDPR; cf. on this already Chapter 2.4.3.3.
419 Commission, European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)), Recital 10 (Amendment 13). Cf. on this already Chapter 2.4.5.2.
420 Recital 44 AVMSD.

vertising, online shopping, etc. This delineation is illustrated by a list of excluded requirements which relate to tangible goods, such as product labelling, safety, product liability or provisions relating to the transport of goods, including the distribution of medicinal products.

The EU may have been aware of the risk that measures set for online service providers inadvertently permeate to other areas beyond the scope of this online-related Directive. An example could be commercial services that just have an electronic component but are otherwise governed by provisions that may fall under a different category of competence according to the EU Treaties.[421]

This close circumscription of the coordinated field may indeed pose further challenges as business models of the platform economy diversify and converge. The pre-eminence of online marketplaces, the rise of sharing economy platforms, the expansion of social media into adjacent markets or the convergence of on- and offline markets are just some illustrations. For example, it may be increasingly confusing to regulate the online advertisement of products through the rules concerning e-commerce while making the requirements relating to the sale of the products subject to product regulation (as detailed in Recital 21).[422] In addition, a number of EU product laws today provide specific rules on the sales of products online, such as product labelling in sales over the Internet.[423]

The ECD also excludes from its scope the field of taxation, cartel law, data protection, activities of notaries, legal representations before courts as well as gambling activities, which includes lotteries and betting.[424]

3.1.3. Personal Scope of Application

The ECD aims to regulate certain aspects of information society services. It refers in Art. 2 lit. a to the definition of information society services as laid

421 A concrete example of such a blurring line is the case CJEU, judgement of 2.12.2010, C-108/09, *Ker-Optika v ÀNTSZ Del-dunántuli Regionális Intézete*. Another more general illustration of this phenomenon is the burring line of sharing economy platforms such as Uber and Airbnb; cf. on these cases below Chapter 3.3.7.3.

422 *Rowland/Kohl/Charlesworth*, Information Technology Law, p. 269.

423 Thus, for example, Art. 5 para. 1 lit. a of Regulation (EU) 2017/1369 of 4 July 2017 sets a framework for energy labelling and repeals Directive 2010/30/EU 2017, OJ L 198, 28.7.2017, pp. 1–23.

424 Art. 1 para. 5 ECD.

down in Art. 1 para. 2 lit. a of the Technical Standards and Regulation Directive.[425] According to this, an information society service needs to be provided "for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[426] Service providers are defined as any natural or legal person providing an information society service.[427] The ECD regulates the activities of these service providers in the coordinated field covered by the Directive. Information society service providers cover a wide field of actors in the digital economy, from Internet retailers and financial services to electronic libraries, file transfer services, and social media and online agencies of various sorts.[428]

The remit of the meaning of the criteria by remuneration, at a distance, by electronic means and at the individual request of a recipient has been interpreted by the CJEU in a number of cases, such as notably *Mediakabel*[429] and *Papasavvas*[430]. More recently, the CJEU was asked whether sharing economy platforms *Uber*[431] and *Airbnb*[432] could be regarded as information society services. These cases illustrate the growing diversity of online business models, which now disrupt regulated, "offline" sectors of the economy. The claim of these services to be regarded as information society services can arguably be attributed to an advantageous regulatory environment for these services in such circumstances, namely the country-of-origin principle and liability exemptions for intermediary service providers.

For *Uber*, using this favourable regime as a market access opener[433] for the EU has not been successful for now. *Uber* had claimed that the electronic component of its ride hiring business was the essential activity, a

425 Supra (fn. 203), Art. 1 para. 1 lit. b. Cf. already above at 2.4.1.1.

426 Art. 1 para. 2 lit. a of Directive (EU) 2015/1535; Recital 17 of the ECD repeats this definition.

427 Art. 2 lit. b ECD.

428 *Büllesbach (ed.)*, Concise European IT Law, pp. 696–698.

429 CJEU, judgement of 02.6.2005, C-89/04, *Mediakabel BV v Commissariaat voor de Media*, in which the CJEU interpreted the meaning of "service provided at the individual request of a recipient".

430 CJEU, judgement of 11.09.2014, C-291/13, *Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis*, in which it elucidated on the meaning of "for remuneration".

431 CJEU, judgement of 20.12.2017, C-434/15, *Asociación Profesional Élite Taxi v Uber Systems Spain SL*.

432 Opinion of Advocate General Szpunar, delivered on 30.4.2019, C-390/18, *YA, Airbnb Ireland UC, Hotelière Turenne SAS, Association pour un hébergement et un tourisme professionnel (AHTOP), Valhotel.*

433 *Hatzopoulos*, The Collaborative Economy and EU Law, pp. 31–32.

view that was not shared by the CJEU. *Airbnb*'s claim was similar to that of *Uber*. However, Advocate General Szpunar came to a different conclusion than for *Uber* by applying the methodology used in that latter case.[434] The criteria for qualifying the status of the service provider are whether the alleged information society service creates a new, stand-alone market and whether it exerts control over the transactions facilitated by the platform.

The rulings provide useful clarification on the concept of information society services and their applicability to new sharing economy platform models, especially where they provide composite (electronic and non-electronic) services.[435]

3.2. The Country-of-Origin Principle

3.2.1. Application

The activities of information society service providers are framed by the country-of-origin principle. Art. 3 para. 1 ECD obliges Member States to ensure that information society service providers which are established in their jurisdiction, the country of origin, comply with the rules of that Member State throughout the EU. In turn the internal market principle (non-discrimination principle) precludes Member States from restricting the freedom to provide these information society services established in another Member State on the basis of their domestic (destination) provisions.[436] As a consequence, the information society services covered by the ECD are subject to the rules of just one Member State: that of the country of origin or where the service provider is established. This relatively clear application of the country-of-origin principle has been attributed to the EU's strong objective to create a harmonised regulatory framework for the then emerging electronic commerce services within the EU.[437]

On the other hand, this strict country-of-origin-rule approach also has its impracticalities, for example when court decisions, such as information requests, need to be enforced against information society service providers,

434 Opinion of Advocate General Szpunar, delivered on 30.4.2019, C-390/18, supra (fn. 432), para. 55–78.

435 For a more detailed analysis: *Savin*, in: Journal of Internet Law 23(3), 2019, pp. 1, 16.

436 Art. 3 para. 1 and 2 ECD.

437 *Rowland/Kohl/Charlesworth*, Information Technology Law, pp. 268–269.

including online intermediaries. Member state authorities are required to direct their requests towards the EU jurisdiction where the entity has its seat of establishment, even if a branch or subsidiary entity may exist in their own country.[438] Likewise, requests for enforcing against a provider would need to be directed towards the authority of the origin Member State or the appropriate regional authority if the enforcement falls under regional competencies. High administrative burdens and a perceived lack of effectiveness in enforcement are drawbacks of this approach. It has therefore been argued that the country-of-origin principle in the ECD creates a conflict of law rule by virtue of pointing towards the law of place of establishment of the ISS provider.[439]

The country-of-origin approach applies to those activities of information society service providers which are covered by the coordinated field of the Directive.

3.2.2. Derogations

Member States have the right to restrict the free movement of information society services under certain conditions. Art. 3 para. 4 ECD creates derogations for situations where Member States deem it necessary[440] for reasons of public policy, public health, public security and consumer protection to apply stricter rules than those provided by the country of origin. The public policy justifications relate to criminal offences, including the protection of minors, the fight against incitement to hatred and violations of human dignity. Beyond the need for a legitimate aim, these measures need to be proportionate.[441]

Member States are held to coordinate with the origin Member States and first ask that state to apply the enforcement measures sought.[442] The destination Member State may only act if the origin Member State did not act on requests made or when the action taken was insufficient. The Com-

438 Administrative Court of Berlin, judgement of 20.7.2017, case 6 L 162.17, para. 33–39. In this case Berlin authorities were refused an order for disclosure of information made to the local subsidiary of *Airbnb* on the grounds that this request would need to be directed at the company's EU seat of establishment in Ireland.

439 *Büllesbach (ed.)*, Concise European IT Law, p. 306.

440 Art. 3 para. 4 lit. a point (i) ECD.

441 Art. 3 para. 4 lit. a point (iii) ECD.

442 Art. 3 para. 4 lit. b ECD.

mission will need to be notified of any derogative measures taken by a destination Member States. It is held to examine any derogative action with an option to request that a Member State stop these measures should they be deemed disproportionate.

The focus on cooperation and the very closely circumscribed conditions for derogations demonstrate the importance that the EU has attached to the country-of-origin principle as a regulatory model in this area. Indeed, the derogations appear to have been used rarely so far.[443] Others have argued that the complexity of the derogations in Art. 3 para. 4 leaves the door open to incision by substantive law at national and EU level.[444]

It may be of interest for regulatory cooperation that the ECD's country-of-origin rule (and with it the derogations of Art. 3 para. 4) has been perceived as being most effective when implemented as a rule of legislative and not adjudicative jurisdiction, i.e. a rule with public law and not conflict-of-laws characteristics.[445]

Nevertheless, the EU may have been aware of the incentive that a rigorously applied country-of-origin principle may provide for legislative forum shopping or circumvention of stricter legislation by individual Member States. Recital 57 recognises the right of a Member State to take measures against a service provider in another Member State if the choice of establishment was motivated by a desire to evade stricter legislation in the former.[446] However, it can also be argued that the acknowledgement of this risk in a Recital is secondary to the more explicit and elaborate provisions of Art. 3 para. 4 ECD and the cooperation requirements of authorities posited in Art. 19 ECD.

Almost twenty years later the EU legislator charged the newly established European Regulators Group for Audiovisual Media Services (ERGA) with reporting and passing non-binding recommendation on "measures addressing the circumvention of jurisdiction" of audiovisual media service and video-sharing platforms within the framework of the AVMSD.[447] Meanwhile it has introduced specific powers for Member States to go against media service providers having demonstrably registered in a Mem-

443 *Savin*, EU Internet Law, p. 59. The intention of these derogations was clarified in: CJEU, judgement of 25.10.2011, C-509/09 and C-161/10, *eDate Advertising GmbH v X and Olivier Martinez, Robert Martinez v MGN Limited*.
444 *Rowland/Kohl/Charlesworth*, Information Technology Law, p. 270.
445 *Savin*, EU Internet Law, p. 60.
446 Recital 57 ECD.
447 Recital 11 AVMSD.

ber State for the purposes of circumventing stricter regulation elsewhere.[448]

3.2.3. Exemptions to the Scope of Application

Art. 3 para. 3 ECD refers to a number of areas (specified in the Annex of the Directive) which are outside of the scope of the coordinated field and, therefore, the country-of-origin principle. These are amongst others intellectual property rights, electronic money transfers, contractual obligations concerning consumer contracts, real estate contracts and unsolicited mail. These areas have been exempted either due to policy preoccupations by Member States or because they are already covered by other EU instruments.[449]

3.3. The Intermediary Liability Regime

3.3.1. Historical Backdrop

The rising problem of illegal and harmful content on the Internet was first addressed by the EU as early as 1996.[450] In its first Communication on this matter, the Commission underlined that Member States remained responsible for applying their national laws to the Internet. However, the risk of diverging responses of national legislators and courts to the role and responsibilities of Internet intermediaries was clearly identified. It could eventually distort competition, hamper the free movement of services and lead to fragmentation of the internal market, the Commission indicated.

At that stage, the EU considered a common EU framework to "clarify the administrative rules and regulations which apply to access providers and host service providers"[451] as a policy option. This was proposed alongside with promoting industry self-regulation and encouraging Member States to cooperate and define minimum standards for criminal content.[452]

---

448 Art. 4 para. 3 lit. b AVMSD.
449 *Savin*, EU Internet Law, p. 58.
450 Commission, Communication from the Commission: Illegal and Harmful Content on the Internet, COM(96) 487 final, 16.10.1996, available at https://core.ac.uk/reader/5078710.
451 Ibid., p. 25.
452 Ibid., pp. 24–25.

The threat of legislative intervention, however, was not hidden in that document.

By late 1998, that "threat" came true in that the Commission had incorporated proposals for an intermediary liability framework into the draft ECD. Several reasons can be assumed. First, the still young intermediary sector did not manage to come up with its own, self-regulatory rules. Secondly, the first national jurisprudence on intermediary liability laid bare diverging interpretations of whether and how intermediaries should be made liable for third-party content.[453] Thirdly, the US had enacted two centrepieces of intermediary liability regulation: the Communications Decency Act 1996[454] and the Digital Millennium Copyright Act 1998[455] (DMCA).

3.3.2. The Approach Chosen by the EU

The EU opted for a broad horizontal framework that did not follow the sectorial approach favoured in the US. It nevertheless borrowed heavily from the US provisions. This is particularly visible in the categorisations and definitions of intermediaries and certain conditions that govern the exemptions from liability. The EU framework is generally considered stricter than that of the US[456] as it expands the more onerous conditions on liability exemptions that the US imposed on intermediaries for copyright violations in the DMCA across all content areas. At the same time, however, it is also less specific.[457] It does not provide any guidance on the process and format of notices and counter-notices, nor does it spell out any "Good Samaritan" protections[458] for those intermediary providers that choose to proactively identify and remove illegal content.

---

453 Three of the most known intermediary liability cases from the UK, Germany and France of that time shall be illustrative of this: *Godfrey v Demon Internet Limited* [1999] EWHC QB 240 (23 April, 1999); *CompuServe [1998]* AG München 8340 Ds 465 Js 173158/95, MMR 1998, 429; *UEJF and Licra v Yahoo! Inc and Yahoo France* (Tribunal de Grande Instance de Paris). Cf. also Recital 40 ECD.

454 Communications Decency Act 1996 (47 USC § 230).

455 Digital Millennium Copyright Act, supra (fn. 197).

456 See for example *Savin*, EU Internet Law, p. 148; *Rowland/Kohl/Charlesworth*, Information Technology Law, p. 93.

457 *Edwards*, The fall & rise of intermediary liability, p. 74.

458 47 USC § 230 section 230 lit. c.

An explanation could be seen in the broad internal market focus of the ECD which does not allow for specifications dependent on substantive "content" law. Secondly, the regulatory choice to approximate laws using a minimum harmonisation approach may have inhibited the EU from putting down more specific procedural detail. Thirdly, one of the *raison d'être* for the liability framework was economic. A broad shield from liabilities for third-party content and a focus on self-regulatory solutions were meant to promote innovation and growth in the Internet economy. Notwithstanding these arguments, the above omissions have been criticised as causing legal uncertainty and hindering the effective removal of infringing content.[459]

3.3.3. Categories of Specific Information Society Service Providers

The EU liability framework does not establish a general liability regime but a system of exemptions for certain activities[460] of those information society services that are classed as intermediary service providers.[461] That latter term is however not set out in the definitions in Art. 2 of the ECD nor in any other EU instrument. Instead, the EU defines intermediary service providers only in relation to the activities that are subject to the exemptions or specific liability rules.

The ECD defines three types of activities for intermediary service providers (cf. already Chapter 2.4.1.3.): "Mere conduit" (Art. 12), "Caching" (Art. 13) and "Hosting" (Art. 14). Art. 15 stipulates additional protections for all three activities. Similar to the DMCA in the US, the ECD introduces a graduated system of liability exemptions for these activities, according to the technical involvement of the intermediary's activity in the intermediation process.

459 *Edwards*, The fall & rise of intermediary liability, pp. 73–77.
460 *Baistrocchi*, in: Santa Clara High Technology Law Journal 19 (1), 2003, pp. 111, 117–118.
461 Section 4 ECD.

Directive 2000/31/EC
Art. 12 Mere conduit
1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. 2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission. 3. This Art. shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement
Art. 13 Caching
1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. 2. This Art. shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Art. 14 Hosting
1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider. 3. This Art. shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.
Art. 15 No general obligation to monitor
1. Member States shall not impose a general obligation on providers, when providing the services covered by Art. 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

The common trait and therefore the defining element of all three types of intermediary service providers is that they process information that is provided by a recipient of the service or by a third party. It is therefore clear that the intermediary liability framework laid down in Art. 12–14 does not deal with scenarios where the information service provider is the originator of the content. The Commission underlined this also in its first application report of the ECD of 2003.[462] This distinction was later on clarified and confirmed by the CJEU ruling in *Papasavvas*.[463] All other conditions stated in Art. 12–15 relate to the availability of the exemption from liability

462 Commission, First Report on the Application of Directive 2000/31/EC 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, (2003) COM(2003) 702 final 12.

463 CJEU, judgement of 11.09.2014, C-291/13, supra (fn. 430).

for the information provided by the recipient of the service. This system of exemptions is also referred to as limitations, immunities or privileges.

The overarching condition for the application of the content liability immunity for all three activities is that they are "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".[464] The reference to knowledge and control implies that truly neutral and passive intermediaries would be immune from any kind of secondary liability, be it vicarious or contributory liability. In many legal systems, vicarious liability is normally allocated to third parties that have control over the actions and behaviour of another party. Contributory liability applies to those agents that have knowledge of infringing acts and are in a position to interfere.[465]

3.3.4. The Three Types of Specific Intermediary Service Activities

3.3.4.1. "Mere Conduits" According to Art. 12 ECD

Mere conduits transmit information through a communication network or provide access to such a network. The passivity of the mere conduit is defined through three conditions, the fulfilment of which qualifies for a full exemption from liability for the content transmitted. The conduit must not 1) initiate the transmission, 2) select the receiver of the transmission and 3) select or modify the information that is contained in the transmission. Art. 12 para. 2 clarifies that this includes transient storage where this happens solely as part of the transmission process and where the information is not kept longer than needed for the act of transmission. These exemptions do not prevent Member States' courts or authorities to issue orders for the termination or prevention of an infringement.[466]

When the ECD was drafted, "mere conduits" were mainly Internet access providers that provided customers with a connection to the wired Internet, using ISDN or (A)DSL dial-up connections. Since then, the variety of mere conduits has diversified in line with new Internet access technologies and the omnipresence of the Internet. Mere conduits today may also

464 Recital 42 ECD.
465 For a more detailed treatment of the subject: *Burk*, in: Philosophy & Technology 24(4), 2011, p. 437.
466 Directive 2000/31/EC (ECD), Art. 12 (3).

be mobile telecommunication service providers, Wi-Fi network access operators or various hotspot providers. These services are run by a huge variety of businesses and institutions from shops[467] or restaurants, transportation companies and hospitals to public authorities and universities.

In general, the proliferation of access providers has not led to more ambiguity over the availability of the protections offered by Art. 12 para. 1 ECD. By contrast, mere conduits have been very much in the focus of courts and authorities to help stop and prevent illegal activities and access to illegal content, according to the possibilities offered by Art. 12 para. 3 ECD. Internet access providers sit at a crucial junction of the Internet connection, which makes them an obvious target of enforcement. Consequently, mere conduits have been in the focus of legal disputes when it comes to the scope and breadth of injunctions for removal of, and prevention of access to, illegal content, especially in the context of the limitations imposed by Art. 15. This issue is one of the major controversial discussion points of the liability framework under the ECD[468] and will be dealt with further below.

3.3.4.2. Caching According to Art. 13 ECD

This provision protects providers from being held liable for cached content on their services.[469] In order to benefit from exemptions of liability of cached content, the intermediary service provider must meet five conditions. These five conditions essentially say that the provider must not interfere with the cached content beyond what is technically necessary and required by industry standards. It includes an obligation to remove or prevent unauthorised content once the provider has gained knowledge that a court or authority has removed that content. In practice, this Article has rarely been in the focus of legal disputes or controversy.

---

467 CJEU, judgement of 15.9.2016, C-484/14, *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH*, para. 43.

468 Commission, Online Services, Including e-Commerce, in the Single Market, A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services, Accompanying the Document, SEC(2011) 1641 final 25.

469 *Lodder/Murray*, EU Regulation of E-Commerce: A Commentary, p. 45.

3.3.4.3. Hosting According to Art. 14 ECD

Art. 14 provides immunities from content liability for all those intermediary service providers that store information provided by a recipient of the service.[470] That recipient is also referred to as third party. The difference to the mere conduit and caching provisions is that the storage or "hosting" of information by these intermediaries is the actual service. It is therefore not transient. Moreover, its duration is determined by the recipient of the service. Normally the recipient of the service needs to rely on an Internet access provider (mere conduit) to access the hosting service in the first place.[471]

The more comprehensive involvement of information hosts in the intermediation process raises the bar for a full exemption from liability. At least one of the following two conditions has to be met, as they are laid down in more detail in Art. 14:

a) the provider does not have actual knowledge of an illegal activity or information on its service or the illegality was not apparent to him; or
b) the provider acted expeditiously by removing or disabling access to the information as soon as he obtained knowledge as in the previous condition.

Actual knowledge implies criminal and civil liabilities while awareness of facts and circumstances only implies civil liability.[472] Art. 14 para. 2 clarifies that the hosting services provider may not avail itself of any liability exemptions if it exercises control over the party that requests the storage of the information. Art. 14 para. 1 and 2 address the two main conditions for secondary liability: knowledge and control. As is the case for mere conduits and caching activities, courts and authorities are able to impose injunctions to terminate or prevent infringements. In addition, Member States may also impose procedures on hosting services on how illegal information needs to be removed or made inaccessible.[473]

Today's intermediary landscape is completely different to what it looked like at the turn of the millennium, when Internet access providers, news-

470 Cf. on the scope of Art. 14 ECD in particular *van Hoboken/Quintas/Poort*, Hosting intermediary services and illegal content.
471 *Büllesbach (ed.)*, Concise European IT Law, p. 331.
472 *Rowland/Kohl/Charlesworth*, Information Technology Law, p. 86; *Lodder/Murray*, EU Regulation of E-Commerce: A Commentary, p. 50.
473 Art. 14 para. 3 ECD.

rooms and the first search engines made up the bulk of Internet intermediaries. Since then e-commerce marketplaces, social media networks, user-generated content platforms and cloud services have appeared, and most of them have been classified as neutral hosts under Art. 14 making them profit from the liability privilege. This change was initiated by the Web 2.0 which allowed for new ways of user interaction and the sharing of content on the Internet. The subsequent rise of Internet intermediaries as key players in global markets and as gatekeepers to information has changed the legal, moral and technical assumptions that underpinned the ECD's liability immunities of the late 1990s. This will be discussed further below.

3.3.4.4. No General Monitoring Obligations According to Art. 15 ECD

Art. 15 para. 1 ECD provides a limitation to Member States' possibilities to oblige intermediary service providers to terminate or prevent infringements. The prohibition of requiring intermediary service providers to monitor the information they transmit or store or to actively search for indications of illegal activity is a necessary limitation if the neutral role of these actors were to serve as a meaningful basis for an exemption from liability. The fear was that any obligation to monitor Internet traffic in a general manner would lead to actual knowledge and a level of control that could invalidate any immunity.

There was also a real concern that any more onerous requirement to monitor the increasing amount of Internet traffic would hamper the development of the young Internet sector.[474] In addition there was a concern that a general monitoring requirement would conflict with the fundamental right to privacy.[475] The interplay between this prohibition and the possibility of courts and authorities to ask for injunction to prevent specific infringements[476] is another aspect of contention of the liability framework of the ECD.[477] On a legal level the debate centred on what the scope of a specific preventive injunction could be that fulfils the criteria of proportionality while being effective.[478] On a purely technical level the dividing

474 *Savin*, EU Internet Law, pp. 161–162.
475 *Büllesbach (ed.)*, Concise European IT Law, p. 333.
476 As provided for in Recital 47 ECD.
477 Commission, SEC(2011) 1641 final, supra (fn. 468), para. 47–51.
478 CJEU, judgement of 12.7.2011, C-324/09, *L'Oréal (UK) Ltd v eBay International AG*, *eBay Europe SARL*, *eBay (UK) Ltd and others*, para. 141; judgement of 3.10.2019, C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*.

line between an injunction targeted at preventing the occurrence of a particular type of violation and the requirement that the entire traffic of the site be monitored has been a subject to intense debate.[479]

Art. 15 para. 2 ECD specifies two obligations for information society providers. Firstly, Member States may establish obligations that public authorities be informed of illegal activities. Secondly, service providers may be obliged to inform authorities of the identity of third parties with whom they have service agreements. However, the latter requirement has been relativised in an early related CJEU judgement in *Promusicae*. The CJEU stipulated that Member States have to balance contradicting fundamental rights of property protection and privacy rights when they decide about a framework in which communication of personal data of users to rights holders would be foreseen.[480]

3.3.5. Delineation between National and EU Responsibilities

The ECD follows a minimum harmonisation approach. This means that in line with the principle of subsidiarity[481] it will only act in areas where it has no exclusive competence if the objectives of the measure can be better achieved through intervention at Union level.[482] Meanwhile the country-of-origin principle allocates the supervisory authority to the Member State where an information society service provider is established.[483] This also extends to the intermediary service providers.

The Directive left it to Member States to define procedures for the removal of, and disabling of access to, illegal information and activity by hosting providers. They are also known as notice-and-takedown procedures.[484] The Directive encourages self-regulatory measures such as voluntary agreements between stakeholders or codes of conduct.[485] The Commission's 2012 evaluation of the ECD found that only a few Member States had either managed to initiate the creation of voluntary agreements

479 *Nolte/Wimmers*, in: GRUR 16(1), 2014), pp. 16, 21–23; *Valcke/Kuczerawy/Ombelet*, Did the Romans Get it Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common, p. 11.
480 CJEU, *Promusicae v Telefónica*, supra (fn. 135).
481 Recital 6 ECD.
482 Art. 5 para. 3 TEU.
483 Recital 22 ECD.
484 Art. 14 para. 3 ECD.
485 Recital 40 ECD.

on notice and takedown or enacted laws to that respect.[486] Where legislations or codes of conduct existed, they did not consistently cover the entire intermediary sector or only applied to certain content areas, such as copyright, child pornography or terrorist content. As a result, a fragmented picture of notice-and-takedown processes emerged, which, according to the stakeholder consultation by the Commission, created legal uncertainty and an obstacle to the Digital Single Market.[487]

The Directive's broad horizontal focus also means that it does not intervene in Member States' provisions in specific content areas. The definition of what is illegal under national law may therefore differ from one Member State to another. For example, defamation is regulated under Member State laws. This is also the case for exceptions and limitations to the reproduction right in EU copyright, which are optional.[488]

While Art. 12–14 give some guidance as to the applicability of criminal and civil sanctions, their applicability is without prejudice to sanctions or remedies according to national law. This means that the breach of intermediary service provider obligations may have different legal consequences depending on the Member State. For example, the approach to contributory liability is determined by Member States' legal traditions, and consequently the kind of sanctions that can be expected by intermediary service providers for the same violation may differ.[489]

3.3.6. Illegal Content – Challenges to EU Intermediary Liability Exemptions

The Commission was obliged by the Directive to re-examine the provisions of the intermediary liability framework with a view to adapt them if needed.[490] The first review of the ECD of 2003 however found that practical experience of the application of Art. 12–14 was still very limited. No court ruling had been issued that originated from cases after the enactment of the ECD.[491] Likewise it found no reason to intervene with legislation in the notice-and-takedown procedures. Four years later the Commission

486 Commission, SEC(2011) 1641 final, supra (fn. 468), para. 40–43.
487 Commission, SEC(2011) 1641 final, supra (fn. 468), para. 43.
488 Cf. Chapter 2.4.4.
489 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries, pp. 34–35.
490 Art. 21 para. 2 ECD.
491 Cf. Commission report on the Application of the ECD, supra (fn. 462), p. 13.

commissioned two studies that dealt with the implementation and impact of the ECD. While one study dealt with the economic imact of the ECD,[492] the other specifically focused on the intermediary liability regime and the interpretation of its provisions by EU Member States and national courts.[493]

This latter study noted diverging interpretations on the liability provisions for host providers by courts. It specifically pointed to unclarity over the term "actual knowledge" in connection with illegal activity and information in Art. 14, para. 1 ECD.[494] Secondly, it noted the variety of injunctions issued against intermediaries. It pointed to an uncertainty and a potential conflict between preventive injunctions against specific infringements, also called staydown orders, and the prohibition to impose general monitoring obligations.[495] The availability of the liability exemptions to intermediaries seemed to be a less prominent issue. However, the report advocated vigilance regarding the emergence of Web 2.0 intermediaries and the potential for conflicting interpretations over the availability of Art. 14 for hosting activities.[496]

The 2012 evaluation of a public consultation on the application of the ECD found a more substantial need for clarification of the intermediary liability framework.[497] In addition to the problems mentioned in the 2007 study, the report now stated that courts had increasingly divergent views on the scope of activities covered by Art. 12–15 of the ECD. Apart from the longer standing problems with the liability of search engines, the report indicated that new Web 2.0 intermediaries, such as video-sharing platforms, e-commerce marketplaces and social networks, had caused substantial legal uncertainty. Yet in its ensuing evaluation of the E-commerce Action Plan the Commission followed the majority of stakeholders and did not undertake to reform the liability provisions of the ECD.[498]

---

492 *Nielsen and others*, Study on the Economic Impact of the Electronic Commerce Directive.

493 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries.

494 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries, pp. 36–47.

495 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries, pp. 50–52.

496 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries, pp. 102–104.

497 Commission, SEC(2011) 1641 final, supra (fn. 468), para. 24–26.

498 Commission staff working document E-commerce Action plan 2012–2015, SWD(2013) 153 final, available at https://ec.europa.eu/information_society/new

By 2016 the EU noted that the availability of illegal and harmful content had become an even more noticeable problem, especially as online platforms occupied an ever more important position in the daily lives of people. However, although acknowledging persisting concerns with regards to the responsibilities of online platforms, it vowed to "maintain the existing intermediary liability regime while implementing a sectorial, problem-driven approach to regulation".[499] The focus would be on reforming provisions regarding the liabilities of intermediaries through a legislative review of copyright and audiovisual media services. This sectorial approach was confirmed by a Communication and a Recommendation to tackle illegal content online, which both called for more responsibilities of online platforms.[500] These initiatives engendered a number of separate sectorial legislative initiatives aimed at addressing the responsibilities of intermediaries, particularly hosting services, without however opening the ECD-framework laid down in Art. 12–15. These initiatives will be discussed in more detail below (cf. also above Chapter 2.4.1).

3.3.7. EU Intermediary Liability Framework – How the CJEU Has Dealt with the Challenges

3.3.7.1. Challenge : The Question of Neutrality of Hosts

In the first five years after of the ECD, there was relatively little controversy over the availability of the liability immunities under Art. 12–15. Initially, the activity of search engines posed a problem to courts in the EU. However, this controversy was settled in the CJEU ruling in *Google France v Luis Vuitton.* The CJEU found that an Internet referencing service provider (i.e. search engine) could avail itself of the immunities provided through Art. 14 for hosting activities if it did not play an active role in the hosting process.[501] It proved, however, much more controversial to find criteria to determine when more interactive Web 2.0 intermediary service providers, or online platforms, acted in a "mere technical, automatic and

---

sroom/image/document/2017-4/130423_report-ecommerce-action-plan_en_42073.pdf, p. 17.

499 Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM/2016/0288 final, pp. 7–9.

500 Cf. on this already in detail Chapter 2.5.3.

501 CJEU, judgement of 23.3.2010, joint cases C-236/08 to C-238/08, *Google France, Google Inc v Louis Vuitton Malletier*, para. 143.

passive" role, i.e. did not play an active role. The premise of their neutral character was increasingly unclear and hence interpreted differently by courts. A number of rulings during the first decade of the new millennium show diverging understandings by, for example, Belgian, French, German, Italian and UK national courts on the activities of e-commerce marketplaces, user-generated content platforms or search engines.[502]

The first two rulings at CJEU level that attempted to clarify this situation were *Google France v Luis Vuitton*[503] and *L'Oréal v Ebay*.[504] Both cases were brought by French trademark owners who alleged amongst others that Google and eBay's activities went beyond a mere passive and technical role of information society service providers. As a result, both claimants charged Google and eBay, respectively, with being directly liable for violating their trademark rights.

In *Google France v Luis Vuitton* the rights holders sought to establish the existence of actual knowledge and control by the fact that Google assisted clients using the AdWords service in drafting the commercial message next to the advertising link and in suggesting keyword combinations that improved the display of their adverts. The adverts in question appeared as "sponsored links" to websites that sold imitations of the rights holders' trademark-protected luxury goods. The CJEU found that a search engine's matching activity of users requests with keywords stored by advertisers and the subsequent display of results did not constitute an active role. However, the drafting of the advertising message which accompanied sponsored links and the selection of advertising keywords connected to this display may indicate such an active role.[505]

In *L'Oréal v Ebay*, which a UK court had referred to the CJEU, L'Oréal wanted to establish eBay's active role through the assistance it provided to sellers in optimising or promoting the display of certain listings. These listings, however, referred to products that violated the trademark rights of L'Oréal. Similar to *Google France*, the CJEU found in *L'Oréal v Ebay* that storage of an offer, setting the terms of service, providing general information to customers and getting remunerated are neutral components of an online marketplace's activity. By contrast, providing assistance to the seller,

502 Commission, SEC(2011) 1641 final, supra (fn. 468), para. 26–30; *Waisman/Hevia*, in: International review of industrial property and copyright law 42(7), 2011, pp. 785 et seq.; *Bertolini/Franceschelli/Pollicino*, Analysis of ISP Regulation under Italian Law, pp. 156–163.

503 CJEU, *Google France v Louis Vuitton*, supra (fn. 501).

504 CJEU, *L'Oréal v eBay*, supra (fn. 478).

505 CJEU, *Google France v Louis Vuitton*, supra (fn. 501), para. 115–119.

such as optimising the display and promoting offers means active involvement and hence forfeiture of the liability exemption.[506] In both cases, the CJEU referred the matter back to the national courts so that they apply these criteria to the concrete facts and circumstances on a case-by-case basis.

These rulings, however, did not appear to have brought the clarity sought. National courts have continued to this day to come to diverging results and classifications of the role of hosting services providers. Prompted by the CJEU, they assessed the role of hosting services according to the criteria laid down by the EU court, but they developed their own methodologies in doing so. This is hardly surprising, given the vast variety of hosting services, different legal traditions and varying degrees of understanding of intermediaries' operations and business models.

In other rulings following these two key judgements, the CJEU had no trouble in allocating the Art. 14 hosting defence to social networking services, such as in *Netlog* (*SABAM v Netlog*[507]) and, very recently, *Facebook*[508]. Although in the latter case the Advocate General simply stated in his Opinion that, "irrespective of the doubts that one might have in that regard"[509], the referring court found that it was common ground that Facebook is a host provider and, by implication, a neutral actor. It is clear that the CJEU sticks to its line by letting national courts elucidate on this issue.

Lastly, the CJEU confirmed its "hands-off approach" in the *SNB-REACT* case by referring the question of whether Internet registries and registrars are neutral intermediary service providers that could qualify for the liability exemptions of the ECD back to the national court.[510] In this case, REACT, an industry association which defends the rights of trademark owners, brought a challenge against an IP address rental and registration service which had registered 38,000 IP addresses and domains that violated the trademark rights of its members.

Despite these rulings the concept of the neutral ("mere technical, automatic and passive") host remains unclear in its application at national lev-

506 CJEU, *L'Oréal v eBay*, supra (fn. 478), para. 115–117.

507 CJEU, judgement of 16.2.2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, para. 27.

508 CJEU judgement *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, supra (fn. 478), para. 22. Cf. further analysis below Chapter 3.3.7.3.4.

509 Opinion of Advocate General Szpunar on *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, delivered on 4.6.2019, C-18/18, para. 30.

510 CJEU, judgement of 7.8.2018, C-521/17, *Coöperatieve Vereniging SNB-REACT U.A. v Deepak Mehta*, para. 47–52.

el.[511] Two current referrals which are pending in front of the CJEU are testimony to this. Both referrals come from copyright owners and seek guidance on the availability of the hosting defence (Art. 14) to the activities of video-sharing platform YouTube. In both cases the claimants had repeatedly notified to YouTube content that infringed their copyright and eventually asked the video-sharing platform to prevent notified content from reappearing (staydown requests). They also claimed that the activities of YouTube went beyond that of a passive host, namely by offering users to search, flag and comment on content, by deriving advertising and licencing revenues, by recommending content to users and by sorting and ranking content. The cases referred by the German and Austrian Supreme courts are still pending.[512]

One solution that has been brought forward in response to the difficulties in deciding whether Art. 14 is available to new Web 2.0 intermediaries is the creation of additional categories of intermediary service providers in the ECD.[513] The risk is that this may be overrun rather quickly by market developments, potentially even before such changes are enacted. In addition, this approach could risk steering away from the technology-neutral focus of the ECD. Others have argued to scrap the distinction between neutral and active hosts altogether,[514] because this assessment is very complex and requires deep technical and operational understanding of the concrete hosting context at hand. It also diverts from the fact that most Web 2.0 intermediaries today profit immensely from the data and information generated by user activity. Claims of being a neutral host sit uncomfortably with the intrusive nature of many of these platforms and the mas-

511 Commission, Synopsis Report on the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries and the Collaborative Economy, available at https://ec.europa.eu/digital-single-market/en/news/synopsis-report-contributions-public-consultation-regulatory-environment-data-and-cloud, pp. 15–16.

512 Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 6 November 2018, *LF v Google LLC, YouTube Inc, YouTube LLC, Google Germany GmbH* (Case C-682/18); Request for a preliminary ruling from Oberster Gerichtshof (Austria) lodged on 1 July 2019, *Puls 4 TV GmbH & Co KG v YouTube LLC and Google Austria GmbH* (C-500/19).

513 Synopsis Report of the Commission, supra (fn. 511), p. 16.

514 *Martens*, An Economic Policy Perspective on Online Platforms, pp. 34–35; *Ullrich*, in: International Journal of Law and Information Technology 26(3), 2018, p. 226, 242.

sive benefits generated from exploiting big data.[515] This way of thinking is also expressed in an early preparatory document of the Commission services concerning a possible future "Digital Services Act", according to which the distinction between active and passive hosts could be given up in the future.[516]

3.3.7.2. Challenge 2: Actual Knowledge

Once intermediary service providers are found to act in a mere technical and passive way, they can avail themselves of the liability exemptions if they do not have actual knowledge of the illegal activity/information or if they remove it expeditiously once they have obtained that knowledge. This requirement is specific to caching and hosting activities[517] and not relevant for the liability for mere conduits.[518] In addition, hosting providers are not allowed to be aware of facts and circumstances from which illegal activity is apparent.[519]

Knowledge is a precondition for finding contributory liability. However, early reports have shown that Member States had implemented these requirements differently into their national law.[520] Even where they followed a literal transposition of the Directive's text, courts had come up with differing interpretations.[521] The consensus that has arisen through national and EU rulings is that there are three ways in which an intermediary service provider can gain that actual knowledge. First, a court order, secondly a notice by an allegedly damaged party and third through awareness over illegal activity and content.

---

515 *Zuboff*, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, para. 2051; *Naughton*, Platform Power and Responsibility in the Attention Economy, pp. 388–389; *Friedmann*, in: Journal of Intellectual Property Law and Practice 9(2), 2014, pp. 148, 150.

516 Cf. the leaked document confirming that DSM Steering Group is engaged in drafting a Digital Services Act that would serve as a basis for a REFIT of the ECD and establish new rules on platforms, available at https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf.

517 Art. 14 para. 1 lit. a and b ECD, and Art. 13 para. 1 lit. e ECD, respectively.

518 CJEU, *McFadden v Sony*, supra (fn. 467), para. 63–65.

519 Art. 14 para. 1 lit. a ECD.

520 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries, pp. 34–47.

521 Commission, SEC(2011) 1641 final, supra (fn. 468), para. 32–36.

On the second point, under receipt of a notice, the intermediary would need to decide on the veracity of the claim and then remove the information expeditiously in order to qualify for the liability exemption. However, since the ECD did not provide any procedural requirements for notice and takedown, the understanding over what constitutes actual knowledge following a notice has differed across the EU. The CJEU has so far not been called up to give guidance on this issue. The Commission is currently reviewing whether there is a need for EU-wide notice-and-takedown processes.[522]

Awareness of illegal activity has been another ambiguous concept. If a provider truly is a passive host, it is unclear how it should become aware of illegal activity or information on its servers. This matter was first addressed by the CJEU in *L'Oreal v Ebay*. The CJEU stated that a sufficiently precise and substantiated notice could result in such awareness.[523] Secondly, a hosting provider could lose its immunity if it did not act on indications of illegal activity that it should have become aware of as a diligent economic operator. This includes voluntary proactive investigative activity by the intermediary.[524] This was the first time that the CJEU referred to duties of hosting providers that go beyond barely reactive responses to notifications. Diligent economic operator principles come close to duties of care, which are optional for Member States to impose on hosting providers,[525] and to principles of corporate responsibility.

Under current EU law this may, however, deter any "Good Samaritan" activity because it does not protect the intermediary explicitly in case of error when actively searching for illegal content or having procedures in place. Unlike the US,[526] the EU has not provided such a protection in its legislation. It has also been argued that this ruling may create a conflict with Art. 15 of the ECD, which prohibits the imposition of general monitoring duties. The fear is that it may force intermediaries to monitor for illegal activity in order to act as a diligent economic operator.[527] It is true that the broad and monolithic prohibition of Art. 15 may be perceived as standing in the way of diligent economic operator principles. However,

522 COM(2017) 555 final (supra fn. 394), p. 4.
523 CJEU, *L'Oréal v eBay*, supra (fn. 478), para. 122.
524 CJEU, *L'Oréal v eBay*, supra (fn. 478), para. 120, 122.
525 Recital 48 ECD.
526 47 USC § 230 s. 230 (c).
527 *Savin*, EU Internet Law, p. 161.

this is not the only possible interpretation, as will be shown in the discussion of the problem in the next section.

There is still a lack of clarity on this approach, as the CJEU has not elaborated further on the diligent economic operator principle in any of the following cases dealing with intermediary liability. The ruling seems to have made an impact however: in the new DSM Directive, efforts of content-sharing service providers to prevent the availability of unauthorised works are to be assessed according to diligent operator principles.[528] The ruling is also used as an argument by the Commission in its Communication on Tackling Illegal Content Online for encouraging the use of proactive measures to detect illegal content.[529]

3.3.7.3. Challenge 3: Preventive Injunctions and Duties of Care

From an early point onwards, Member States have taken the opportunity provided in the ECD to impose on intermediary service providers injunctions to terminate and prevent infringements.[530] Courts and authorities have tried to impose so-called staydown orders, which seek to ensure that information successfully blocked once would not be reposted. Secondly, authorities and courts also sought to order intermediary service providers to prevent similar or even all sorts of infringements in the future.

Very quickly these cases were countered by intermediaries who claimed that this imposed *de facto* obligations to monitor information on a general basis and would therefore contradict Art. 15 ECD. It was initially argued that staydown orders necessitated general monitoring, since in order to detect a re-upload the intermediary would be required to monitor the entirety of its traffic. The counter argument was that staydown orders were specific to the information already notified and therefore did not require general but only a closely circumscribed monitoring, which was therefore au-

528 Cf. Recital 66 of DSM Directive.

529 COM(2017) 555 final (supra fn. 394), para. 11–13. In addition it has been used as guidance to complement provisions for traders that are online marketplaces in the Unfair Commercial Practices Directive: Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices SWD(2016) 163, pp. 123–127.

530 Art. 12 para. 3, Art. 13 para. 2 and Art. 14 para. 3 ECD.

thorised under ECD.[531] The same was eventually argued for the prevention of similar infringements.[532]

A large part of the confusion in this debate centres around the definition of the term "monitoring", which is left aside by the ECD. The fact that prevention and filtering techniques have become more effective and less intrusive has also played into this debate.[533]

3.3.7.3.1. L'Oréal v Ebay (C-324/09)

The CJEU addressed this problem first in *L'Oréal v Ebay.* It confirmed that an injunction must not result in the monitoring of all data in order to prevent any future intellectual property infringements. This would be irreconcilable with the ECD and the IP Enforcement Directive[534]. Notwithstanding these limitations, any measures taken had to be effective and proportionate. Therefore, if the hosting provider did not act on its own initiative to prevent infringements of the same kind by the same seller, it could be ordered by a court to do so.[535] With this the CJEU defined specific preventive orders as acceptable where they were aimed at preventing the same kind of infringement by the same originator (seller). In addition, an online market place may be ordered to make it easier to identify its customer-sellers in order to give damaged persons a right to an effective remedy, while balancing it with other rights as laid down in *Promusicae*.[536]

531 Recital 47 ECD.

532 For a discussion over the years: *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries, pp. 50–52; Commission, SEC(2011) 1641 final, supra (fn. 468), para. 25–26; Synopsis Report of the Commission, supra (fn. 511), pp. 18–19.

533 *Angelopoulos*, European Intermediary Liability in Copyright. A Tort-Based Analysis, pp. 473–474; *Edwards/Veale*, in: Duke Law & Technology Review 16(1), 2017/18, pp. 18, 82.

534 Art. 3 of Directive 2004/84/EC; CJEU, *L'Oréal v eBay*, supra (fn. 478), para. 139.

535 CJEU, *L'Oréal v eBay*, supra (fn. 478), para. 141.

536 CJEU, *L'Oréal v eBay*, supra (fn. 478), para. 142–143.

3.3.7.3.2. Scarlet Extended (C-70/10) & Netlog (C-360/10)

Two important subsequent cases in this matter were brought by the Belgian music authors and rights holder association (SABAM) against an Internet access provider (Scarlet Extended) and an Internet host (the social networking site Netlog).[537]

In both cases SABAM tried to impose an obligation that these intermediaries prevent the unauthorised making available of works in its repertoire through the services of these intermediaries. In *Scarlet Extended* the Internet access provider was asked to filter any peer-to-peer traffic of its subscribers through which works for which SABAM collected the copyright licence were shared. In *Netlog*, the association required that social network users be prevented to share any works that were under the license of SABAM. Both orders would have resulted in the intermediaries monitoring the entire traffic on their systems indiscriminately. Both requests were struck down by the CJEU as disproportionate and irreconcilable with the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information and in violation with the general monitoring prohibition of Art. 15 para. 1 of the ECD.[538]

In *L'Oréal v Ebay* the CJEU defined the acceptable scope of a specific preventive injunction in the light of the general monitoring prohibition on the one hand and the duties of intermediaries to prevent infringing activities[539] on the other. The two cases of *SABAM* provided guidance on the balancing acts involved in broader and indiscriminate preventive injunctions.

3.3.7.3.3. McFadden (C-484/14)

The *McFadden* case dealt with the acceptable scope of preventive measures by another type of provider, a mere conduit which was offering a public Wi-Fi network. This case shed some light on the acceptable preventive measures an Internet access provider could be expected to take to deter infringing activity, in this case copyright violations, by users of its (free) service.

---

537 CJEU, judgement of 24.11.2011, C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*.

538 Ibid., para. 53; CJEU,*SABAM*, supra (fn. 507), para. 51.

539 Recitals 40, 45 ECD.

The CJEU had to choose between three measures suggested by the referring court: the filtering of the entire traffic, the disconnection of the network connection and password protection of the Wi-Fi network. The court decided that only the third measure was proportionate. Requiring from a Wi-Fi network provider that its users sign up to the service by revealing their identity was deemed a proportionate means of deterring unauthorised use of the network.[540] This ruling confirmed that preventive measures such as customer identification are adequate obligations that could be imposed on intermediaries as part of a duty of care, at least were intellectual property protection is concerned.[541]

3.3.7.3.4. Eva Glawischnig-Piesczek v Facebook Ireland (C-18/18)

The jurisprudence on the scope of preventive activity filtering was further refined and extended in the recent *Facebook* case.[542] The CJEU was asked whether the social network could be obliged to suppress repeated instances of defamatory comments made against the Austrian politician Eva Glawischnig-Piesczek. The case dates back to 2016 when the former member of the Austrian Parliament and spokeswoman of a party was confronted with insulting and defaming comments on her Facebook page, following an Article she had written about the refugee situation in Austria. That comment, which was publicly accessible to all users, also contained a photo of the politician posted by the commenting user. Facebook declined to follow Glawischnig-Piesczek's request to remove the comments and photograph of her. The politician finally succeeded in a prohibitory injunction, in which it asked Facebook to cease and desist from disseminating any photographs of her that showed accompanying text identical or equivalent to the original insulting comments.

Both parties went through successive appeals stages and arrived at the Austrian Supreme Court (Oberster Gerichtshof). That court was asked to whether it was proportionate to place an order against a social network that extended to preventing identical statements or those with an equivalent meaning to the original harmful comments. The Supreme Court, aware of the EU law ramifications at stake, turned to the CJEU for guid-

---

540 CJEU, *McFadden v. Sony*, supra (fn. 467), para. 90–98.

541 *Ullrich*, in: International Journal of Law and Information Technology 26(3), 2018, p. 226, 243–244.

542 CJEU, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, supra (fn. 478).

ance, essentially requiring clarification on the scope of a staydown order: could it include the same comments and extend to equivalent comments? What was the limit of the prohibition on general monitoring obligations imposed by Art. 15 of the ECD? This case can be seen as a major chance for clarifying the acceptable scope of preventive obligations of social networks classified as hosting providers under the ECD. In other words, they provided the CJEU with an opportunity to shed light on when a specific prevention duty was turning into a disproportionate, general monitoring obligation.

The CJEU ruled that Facebook could be obliged to accept a staydown order for identical comments made by any user of the network against the politician in question. In addition, it could be asked to prevent equivalent defamatory comments from the same user, provided the difference in the content did not require Facebook to engage in an independent assessment. The comments would have to be made inaccessible for all users within the EU, while leaving it open to the Member State to decide on whether this duty could be extended globally in the context of the applicable international law.

The ruling has been interpreted as an endorsement of automatic filtering techniques as means of qualifying for the immunities of Art. 14 of the ECD.[543] The Court stated that, in the light of the availability of automated search tools and technologies, the staydown obligation would only extend to equivalent content for which the service provider would not need to make an independent assessment.[544] This is also supposed to affirm the purely technical, passive and automatic character of the activity. However, it also shows the problems of not having any "Good Samaritan" protections in place. The intermediary's preventive activity is limited to the strict necessary extent if it wants to protect its "neutral" status. The Advocate General had usefully distinguished in his opinion on this case between preventing infringements in intellectual property, as laid down in *L'Oréal v Ebay*, and in defamation cases.[545] The implication in this case is that the

543 *Keller*, Filtering Facebook: Why Internet Users and EU Policymakers Should Worry about the Advocate General's Opinion in Glawischnig-Piesczek' (*Inforrm's Blog*, 7 September 2019) https://inforrm.org/2019/09/08/filtering-facebook-why-internet-users-and-eu-policymakers-should-worry-about-the-advocate-generals-opinion-in-glawischnig-piesczek-daphne-keller/.

544 CJEU, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, supra (fn. 478), para. 46.

545 Opinion of Advocate General Szpunar on *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, supra (fn. 509) para. 68–69.

use of automatic filtering tools for preventing the same and equivalent infringements in defamation cases is classed as a specific prevention obligation, which is incompliant with Art. 15 ECD.[546] This seems to be in line with the recent endorsement of the EU lawmakers for the use of automated filtering technology by Internet intermediaries in order to prevent specific infringements and illegal activity[547], at least as long as the general monitoring prohibition is in place.

However, one of the potential problems is the broad horizontal focus of the ECD. As shown above, the scope of preventive or more far-reaching duty of care obligations may depend on the violations at stake. The balancing act required may lead to varying outcomes depending on whether IP rights, personality rights such as defamation, public security or other interests are at stake. The scope of preventive duties may therefore vary depending on whether hate speech, copyright breaches, defamatory comments, counterfeit sales, child pornography or illegal or unauthorised products are at stake. A larger Internet host may have to deal with all or some of these issues at the same time and would need to adjust its responsibilities to the type of content involved.

3.3.7.4. Other Intermediary-Related Case Law

There are a number of other cases which are usually evoked when talking about intermediary liability law but have not been analysed here so far. *Pirate Bay*, *GSMedia* and *Telekabel*[548] all concern copyright breaches that are facilitated by the use of intermediaries (Internet access providers or hosting services). In all three cases the Advocate Generals evoked the enforcement options against intermediaries that are available for rights holders under the liability provisions of the ECD.[549] They did so alongside considering the options offered by the InfoSoc and IP Enforcement Directives

546 CJEU, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, supra (fn. 478) para. 45–47.

547 COM(2017) 555 final, supra (fn. 394), pp. 14–15.

548 CJEU, judgement of 14.6.2017, C-610/15, *Stichting Brein v Ziggo BV and XS4All Internet BV*.

549 Opinion of Advocate General Szpunar, delivered on 8.2.2017, C-610/15, *Stichting Brein v Ziggo BV and XS4All Internet BV*, para. 67, 60, 83; Opinion of Advocate General Wathelet, delivered on 7.4.2016, C-160/15, *GS Media BV v Sanoma Media Netherlands BV, Playboy Enterprises International Inc, Britt Geertruida Dekker*, para. 86; Opinion of Advocate General Cruz Villalón, delivered on

(IPRED)[550] to issue injunctions against intermediaries for facilitating IP rights violations. In all three cases the Court's judgement entirely sidelined the reasoning of the Advocate Generals on the ECD and instead focussed exclusively on applying the remedies offered by the InfoSoc Directive and IPRED. This may have been a precursor to the provisions in Art. 17 of the Copyright Directive: the Court was preoccupied with clarifying first whether these intermediaries could be charged for primary copyright breach. The implication is that a finding of primary liability would automatically exclude protections and remedies available under the ECD.[551] If an intermediary was found to engage directly in acts of communication to the public, this would remove the foundation of the liability exemptions which protect passive hosts that have no editorial control or influence over the content they host.

3.3.8. Defining a "Duty-of-Care" Standard

3.3.8.1. The Reasoning behind New Responsibilities for Internet Intermediaries

In recent years, the call for a review of the current liability immunities towards enhanced duties of care for information hosts (under Art. 14) have become more frequent and vocal. One argument is that the broad and far-reaching liability protections stem from a time when these actors needed to be protected from legal uncertainty and liabilities. Primary or more readily available secondary liability for content could have hampered the emerging Internet and commercial activity therein. It would have put an undue burden on these intermediaries to monitor, filter and arbitrate information posted, especially when technology was less advanced.

These circumstances have changed. Today Internet intermediaries are more than just normal economic actors. Some of them have become powerful corporate actors with far-reaching control over both content and the infrastructure of the Internet. The control over content and infrastructure has conferred on them gatekeeping powers which would call for en-

---

26.11.2013, C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, para. 52, 77, 78.

550 Art. 8 para. 3 InfoSoc Directive; Art. 11 IPRED.

551 For a more detailed review: *Rosati*, in: European Intellectual Property Review 39(12), 2017, p. 737, 737 et seq.

hanced responsibilities. In addition, the increasing amount of data shared via these intermediaries is exploited and monetised in unprecedented ways. This further questions the merely technical, automatic and passive character of the activities of intermediaries, which is, however, the preconditional criterion for the far-reaching immunities they currently enjoy.[552]

In line with the emergence of powerful Web 2.0 platforms, there have been increasingly calls for enhanced responsibilities alongside so-called duties of care to be imposed on Internet intermediaries. The rationale is that increased powers also justify increased responsibilities. There is a tendency away from the traditional liability framework towards responsibility. The justifications are both of a moral and economic nature.[553] In essence they see new obligations according to the model of corporate responsibility imposed on the intermediaries. A number of theories and suggestions that explore these enhanced responsibilities use the doctrine of duty of care as an underlying concept. Duty of care is common to many legal systems. In tort law it is defined as "a legal obligation imposed on an individual to avid foreseeable harm to others by taking reasonable care".[554] As a framework that defines a standard of responsibility, it lends itself notably to more complex economic and socio-economic contexts that require factual and technical expertise. This is especially the case where pure verification on legal merits is fraught with difficulties.[555] The scope of duty of care obligations often comprises procedural aspects, such as decision-making procedures or risk management.[556] A failure to observe duties of care can lead to liabilities that can be compared to those resulting from negligence and may result in criminal or civil penalties depending on the type of harm caused.

---

552 These books give more detail on the power and influence of intermediaries within the internet and daily life in general: *Moore/Tambini (eds.)*, Digital Dominance – The Power of Google, Amazon, Facebook, and Apple; *Wagner*, Global Free Expression – Governing the Boundaries of Internet Content; *Zuboff*, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.

553 *Taddeo/Floridi*, in: Science and Engineering Ethics 22(6), 2016, p. 1575; *Helberger/Pierson/Poell*, in: The Information Society 34(1), 2018, p. 1; *Valcke/Kuczerawy/Ombelet*, Did the Romans Get it Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common.

554 *Waisman/Hevia*, in: International review of industrial property and copyright law 42(7), 2011, p. 785, 790.

555 *Hofmann*, Delegation, Discretion and the Duty of Care in the Case Law of the Court of Justice of the European Union.

556 *Rhee*, in: Notre Dame Law Review 88(3), 2013, p. 1138, 1147–1150.

3.3.8.2. Proposals for a "Duty of Care"-Approach

The idea of using the duty-of-care principle for obliging online platforms to participate in more proactive infringement prevention is not new. Several authors have by now explored it. In essence these proposals look at allocating responsibilities to platforms that result in a) them taking *ex ante* account of the risks that exist on their systems with regards to illegal content and activity, b) deploying measures to address these risks, c) ensuring that risk assessment and risk responses are conducted in a transparent way. Some of the more substantial proposal in this area shall be briefly portrayed below.

Helman and Parchomovsky[557] and *Verbiest, Spindler and Riccio*[558] have developed the idea of technology-based safe harbours, where duty of care is tied to the use of state-of-the-art filtering and prevention technology used by intermediaries. Both suggest co-regulatory solutions, namely technical standardisation, to create statutory oversight over the development and use of these technologies. *Helman and Parchomovsky* have developed a proposal specific to the prevention of copyright violations on Internet platforms. *Verbiest, Spindler and Riccio* propose the EU New Approach towards standardisation as a (co-)regulatory model. Intermediaries would be required to use that preventive filtering technology against repeat infringements, which has been mandated through technical standards. The aim is to ensure a level playing field between intermediaries and transparency over the content-management decisions, such as filtering algorithms. The application of the New Approach and technical standards to the platform economy have also been taken up by *Busch.*[559] He showcases his solution through the development of an ISO standard for online reviews.[560]

Valcke et al. look at (self-regulatory) codes of ethics as for example drawn up by press associations or journalism councils as a possible model for a duty-of-care standard. These standards would be used by courts as a yardstick when adjudicating on content liability disputes involving ISPs.[561]

---

557 *Helman/Parchomovsky*, in: Columbia Law Review 111(6), 2011, p. 1194, 1225.

558 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries, pp. 19–23.

559 *Busch*, in: Journal of European Consumer and Market Law 6(6), 2017, p. 227.

560 Technical Committee ISO/TC 290, ISO 20488:2018, Online consumer reviews – Principles and requirements for their collection, moderation and publication, available at https://www.iso.org/standard/68193.html.

561 *Valcke/Kuczerawy/Ombelet*, Did the Romans Get it Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common.

Waismann et al. have proposed a flexible standard of duty care for search engines, which is based on reasonableness. That reasonableness would be dependent on scope, cost, harm and impact on fundamental rights.[562] *Woods and Perrin*[563] have so far made the most detailed proposal for a statutory duty of care, which is at the heart of a recent UK Government White Paper to deal with the harms caused by illegal and unacceptable content on social media.[564] This proposal ties the preventive and reactive activities by intermediaries to the *ex ante* definition of key harms that content on these platforms causes to society. They base their approach on the theory that today's social media platforms are public spaces and therefore have special responsibilities to protect users who enter these spaces. Parallels to this regulatory approach can be found in EU health and safety, environmental protection and data protection regulation, amongst others. The proposal is, however, open about whether self- or co-regulation should be used to implement their solution.

Ullrich[565] has proposed a duty of care standard along a technical compliance framework that obliges platforms to deploy a risk-based approach towards the identification and removal of illegal content, similar to approaches used in fraud detection. The conceptual framework follows that of *Woods/Perrin, Verbiest/Spindler/Riccio* and *Busch*. The definition of public interests that platforms need to safeguard (equivalent to the definition of harms) is translated into essential technical and procedural requirements that these platforms need to fulfil as responsible actors. Compliance with these essential requirements could be achieved through a technical standard. Meeting this standard would be considered as a safe harbour from liability. The regulatory model relies on co-regulation and takes the New Approach as a blueprint. Enforcement could either be achieved through national regulators or other cooperative forms of regulatory work on EU level.

What most of these standards have in common is that the traditional distinction between active and neutral hosts would become obsolete or at

562 *Waisman/Hevia*, in: International Review of Industrial Property and Copyright Law 42(7), 2011, p. 785.

563 *Perrin/Woods*, Reducing Harm in Social Media through a Duty of Care; *Woods*, in: InterMEDIA 46(4), 2018/19, p. 17, 17 et seq.

564 Great Britain and Media and Sport Department for Culture, Online Harms White Paper, 2019, available at https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

565 *Ullrich*, in: International Journal of Law and Information Technology 26(3), 2018, p. 226, 226 et seq.

least less important. Instead, emphasis is put on enhanced responsibilities that are proportionate to the involvement in the intermediation process and the risk exposure to illegal activity. The proposals take account of the type of content, the corporate power and the essential functionality that these intermediaries occupy in people's everyday life. However, it should be stated that there are also views that the current intermediary framework is fit for purpose and does not need to be changed.[566] Commentators point out that a further "responsibilisation" of intermediaries might lead to more opaque private speech regulation on the Internet.[567]

3.3.8.3. Illegal Content, Technical Standards and the New Approach

Most of the above proposals focus on establishing responsibility and transparency on the content management decisions taken by online platforms. The idea is that public oversight is established over how the commercial interest in content and data exploration is reconciled with the protection of public interests and fundamental rights.

One solution could be the mandating of European standards bodies to create a technical standard for duty of care regarding the various types of illegal and infringing content. Possible models could be existing principles applied in IT Security (ISO 27000), Occupational Health and Safety (ISO 45001), product standards or even transaction risk monitoring in anti-money laundering.[568] Such a standard would lay down the technical and procedural requirements for ensuring that online hosts prevent and remove illegal content in line with the public interest. These public interest principles would be set out in sector-specific legislation. Compliance with such technical standards would provide proof of conformity with an acceptable level of duty of care and immunity from content liability.

The abovementioned methodology already exists within the EU: the New Approach is a tried and trusted regulatory solution, in which indus-

566 For example: *Savin*, EU Internet Law, p. 173; and *EDRi*, Open Letter on Intermediary Liability Protections in the Digital Single Market, 28 April 2015, available at https://edri.org/open-letter-on-intermediary-liability-protections-in-the-digital-single-market/.

567 *Belli/Sappa*, in: JIPITEC 8, 2017, p. 183; *Frosio*, in: Northwestern University Law Review 112, 2017, p. 20.

568 Cf., e.g., *Perrin/Woods*, Reducing Harm in Social Media through a Duty of Care; *Ullrich*, in: International Journal of Law and Information Technology 26(3), 2018, p. 226.

try-led standardisation is a key component and could potentially be adapted to the problem at hand.[569] It has been considered one of the success stories of European integration.[570] Meanwhile, the EU has continuously reformed its standardisation policy and committed to expand it to the Digital Single Market.[571] Standards could be adopted on a sectorial level to different types of platforms and content, eventually covering the entire ISP sector. Platforms would need to overhaul their risk management activities, making legal compliance a core element of their commercial risk management. The regulator would have authority to review the content (risk) management choices and processes of these platforms and test whether public interest criteria are being respected.

Co-regulation also means that the process of standard creation would be managed by industry, but regulators would be involved in this process and oversee whether the public interest criteria are being adequately reflected in the standard design and implementation. This would entail the review of and involvement in major decisions, from algorithm design of infringement detection and removal systems to procedural arrangements for notice and takedown or statutory reporting. Duty of care is, therefore, not only focussed on preventive actions. A holistic system would also ensure that procedural rights are being observed. It would prescribe formal notice and takedown as well as automated takedown procedural requirements, such as for example the content of notifications, processing times, information requirements to users and counter claim procedures. The standard would also prescribe regular and harmonised statutory reporting by platforms to the public and to regulatory authorities, with some information only being accessible to the regulator.

3.3.8.4. Duty of Care for Internet Intermediaries in the EU Framework

Recital 48 of the ECD gives Member States the option to impose reasonable duties of care on intermediary service providers in order to detect and

569 *Quintel/Ullrich*, Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, Related Initiatives and Beyond, pp. 18–19.

570 *Van Gestel/Micklitz*, in: Common Market Law Review 50(1), 2013, p. 145, 156–157.

571 Commission Communication on ICT Standardisation Priorities for the Digital Single Market, COM(2016) 176 final, available at https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market.

prevent certain illegal activities. It is not clear whether Member States have made concrete use of these provisions. Courts in EU Member States have, however, since the start of the ECD made use of the duty-of-care doctrines in their national laws when adjucating on content liability questions regarding intermediaries.[572]

The first calls for more formalised duties of care to be imposed on intermediaries have arisen out of public consultations.[573] They have mainly been voiced by holders of intellectual property rights and parties interested in the protection of children's rights, product safety or combating hate speech. However, the consultations also show that stakeholders have a different understanding of the scope of duties of care. Intermediaries themselves tend to limit duty of care to the fulfilment of notice-and-takedown obligations and purely voluntary engagements. Other parties tend to extend this to proactive mechanisms of identifying and preventing harms and violations, which could be imposed as obligations.[574]

The Commission has so far referred sparingly to duty of care in its policy documents, although a 2017 European Parliament study has taken up this concept.[575] Nevertheless, the repeated intention to encourage and mandate more proactive measures that platforms should take to fight illegal content can be seen as a readiness to consider that platforms may step up their responsibilities in the fight against illegal content. This shines clearly through in the 2016 Communication on Platforms in the Digital Single Market, where the Commission vows to encourage more proactive, voluntary measures by platforms to fight illegal content and to review the need for formal notice-and-takedown procedures.[576]

---

572 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries, pp. 58–61, 100.

573 Cf. 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), available at https://ec.europa.eu/information_society/newsroom/image/document/2017-4/consultation_summary_report_en_2010_42070.pdf; Synopsis Report of the Commission, supra (fn. 511), p. 19; as well as the Commissions' Summary of Responses to the Public Consultation on the Evaluation and Modernisation of the Legal Framework for IPR Enforcement, 2016, available at http://ec.europa.eu/DocsRoom/documents/18661, pp. 36–39, 50–52.

574 Synopsis Report of the Commission, supra (fn. 511), pp. 19–20; Summary Report IFPR enforcement, ibid., p. 44.

575 *Sartor*, Providers Liability: From the eCommerce Directive to the future.

576 COM(2016) 288 final, supra (fn. 499), p. 9; *Helberger/Pierson/Poell*, in: The Information Society 34(1), 2018, p. 1, 11.

Both the 2017 Communication and the subsequent Recommendation one year later (cf. also above Chapter 2.5.3) aim at clarifying the role of intermediary service providers at tackling illegal content. There is a stronger commitment towards encouraging platforms to take more proactive responsibilities. However, any binding and mandatory measures on proactively identifying illegal content and being involved in its prevention do not seem to be part of overarching horizontal efforts. Rather, the Commission hinted at making this kind of activities binding through sectorial legislation, such as harmful and illegal content in audiovisual media services or for copyright violations.[577] Meanwhile, in the Recommendation online service providers are held to act in proportionate and diligent manner when it comes to identifying and removing illegal content.[578] Here, too, a stronger emphasis on proactive measures to be taken by intermediaries is noticeable.[579] Still, so far the Commission initiatives are limited to non-binding commitments at a horizontal level.

3.3.9. Intermediary Liability Provisions in Sectoral Legislation

As exposed above (Chapter 2.4), there are numerous legislative acts of the EU that deal with some form of responsibility of service providers for content disseminated by them, irrespective of whether it was created by the provider itself. The provisions introduced there are reviewed in the following in order to compare them with the approach taken by the ECD on liability and are supplemented by some further examples of provisions outside of the Digital Single Market context.

3.3.9.1. Sectoral Provisions in Digital Single Market Acts

3.3.9.1.1. Audiovisual Media Services Directive

The Commission had announced an update of the AVMSD as part of its Digital Single Market strategy in 2016. The revised AVMSD was one element of its sectorial, problem-driven approach aimed at putting new provi-

577 COM(2017) 555 final, supra (fn. 394), p. 12.
578 Commission Recommendation on measures to effectively tackle illegal content online, supra (fn. 395), Recitals 17, 27.
579 Ibid., para. 18, 36, 37.

sions in place to protect minors from harmful and illegal content on VSPs. For that purpose, VSPs had to be brought within the scope of the updated AVMSD. However, VSPs are habitually qualified as intermediary service providers and therefore subject to the liability immunities of the ECD. The new AVMSD therefore needed to impose new obligations on these VSPs to deal with illegal and harmful content that respect the framework of the ECD's Art. 14 and 15. Indeed, Art. 28a and 28b, which create new provisions applicable to VSPs, ensure that the measures imposed apply without prejudice to the liability provisions of the ECD.[580]

VSPs are held to protect minors from specific content and fulfil other requirements applying to commercial communications. In addition, Member States are obliged to ensure that VSPs take appropriate measures that shall be "determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created or uploaded the content as well as the general public interest"[581].

These obligations impose a de facto duty of care on VSPs. Having to gauge protective measures to the content in question, the harms, and the user rights and interests at stake does require an *ex ante* risk assessment. Following that assessment, the VSP would then need to take preventive measures that target the risks they have identified. The legal text proposes some of these measures that VSPs would be expected to take. These include flagging and reporting mechanisms, age verification systems, content rating or parental control systems.[582] Member States need to ensure that these measures are being applied by VSPs.[583] On a practical level this means national regulators should be in a position to judge on the adequacy of the risk assessment and the proportionality of the risk responses developed by VSPs.

Despite these comprehensive provisions, the limitations imposed by the general monitoring prohibition of Art. 15 ECD remain in place. The text warns against measures put in place by platforms leading to "ex-ante control measures and upload filters".[584] This is supposed to warrant against any indiscriminate filtering and content suppression by platforms. In prac-

580 Art. 28a para. 5, Art. 28b para. 1 and 3, Recital 48 AVMSD.
581 Art. 28b para. 3 sentence 1 AVMSD.
582 Art. 28b para. 3 sentence 7 AVMSD.
583 Art. 28b para. 3 sentence 2 AVMSD.
584 Art. 28b para. 3 sentence 2 AVMSD.

tical terms, a proper risk assessment by the VSP and subsequent focus on the specific risks in the context of the harms identified by Art. 28b para. 1 AVMSD should not result in general monitoring. The support of co-regulatory measures (along self-regulation)[585] fits within the Digital Single Market framework. It would be an opportunity for the European Regulators Group for Audiovisual Media Services (ERGA) to drive the creation of industry standards around the abovementioned measures prescribed by the AVMSD.[586]

Overall Art. 28a and 28b constitute a comprehensive substantiation at sectorial level of the conditions VSPs need to meet before they can avail themselves of the immunities offered by the ECD. Critical points are that regulators will need to be careful not to impose measures that stray into conflict with Art. 15 ECD and that the AVMSD covers only VSPs in its extended scope. If the same content and harms are found on other types of intermediary service providers, a different regulatory scheme may apply. This may lead to unnecessary legal fragmentation. Therefore, it is important to clarify at least what determines an essential functionality of a service which then in turn allows that service – e.g. a social media service – to be qualified as VSP if that functionality is the sharing of videos. Insofar the Commission guidelines that will be issued in this respect will have an important impact.[587]

3.3.9.1.2. DSM Directive

The recently passed DSM Directive supplements the ECD liability provisions. The newly defined category of online content-sharing service provider clearly targets profit-making user-generated content platforms (including VSPs) and peer-to-peer networks that are in direct competition with online streaming services for audio and video content.[588]

---

585 Art. 28b para. 2 sentence 4 AVMSD, Recitals 49, 58.

586 Art. 30 AVMSD.

587 Cf. further on this *Cole*, Guiding Principles in establishing the Guidelines for Implementation of Article 13 (6) AVMSD; *Weinand*, Implementing the EU Audiovisual Media Services Directive, pp. 666 et seq.

588 Art. 2 para. 6 and Recital 62 DSM Directive: not-for-profit online encyclopedias, not-for-profit educational and scientific repositories, open source software-developing-and-sharing platforms, online marketplaces and business-to-business cloud services are explicitly excluded from the definition.

In contrast to the revised AVMSD, the new DSM Directive interferes directly with the availability of the liability immunities in the ECD. It denies any content-sharing service provider that gives the public access to copyright-protected works uploaded by its users the immunities offered in Art. 14 para. 1 ECD.[589] According to the interpretation of EU copyright law, these providers engage in direct acts of publication or reproduction and would therefore incur primary liability for copyright breaches. This appears to be in line with recent case law of the EU, such as for example in *Pirate Bay*[590].

As a result, the bulk of user-generated content platforms, such as YouTube, Dailymotion and arguably also Facebook, which had been at the centre of copyright holders' discontent, would find themselves outside the safe-harbour protections for these kinds of activities. One could stop the analysis here since the intermediary immunities of the ECD are not any longer available for these platforms. Nevertheless, a review of the measures online-content-sharing providers need to take in order to avoid primary liability for copyright violations shall still be of interest.

Art. 17 para. 1 DSM Directive obliges these intermediaries to obtain the authorisation of the rights holders for copyright-protected content, for example by concluding licensing agreements. Where an authorisation was not available, the provider would need to prove that they have made best efforts to obtain such an authorisation, prevent the availability of unlicensed content according to professional diligence standards and remove it expeditiously upon reception of a notice.[591] This provision requires content-sharing providers to act essentially as diligent operators.

The providers' efforts shall be judged by taking into account its size and business model as well as the cost and availability of suitable means to prevent unlicensed content.[592] It has been argued that these measures *de facto* impose automated filtering systems (upload filters) on providers due to the sheer amount of content hosted by these platforms.[593] If that is true, than the measures go beyond the wide-reaching proactive obligations which the legal framework would likely have prevented to impose under the current

589 Art. 17 para. 1 DSM Directive.
590 CJEU, judgement of 25.4.2017, C-527/15, *Stichting Brein v Jack Frederik Wullems*; *Rosati*, in: European Intellectual Property Review 39(12), 2017, p. 737, 737 et seq.
591 Art. 17 para. 4 DSM Directive.
592 Art. 17 para. 5 DSM Directive.
593 *Henrich*, Nach der Abstimmung ist (fast) vor der Umsetzung; cf. already Chapter 2.4.4.2.

Art. 15 ECD. Still, one could argue that in the AVMSD the legislating bodies of the EU found an acceptable way around this.

The AVMSD and the DSM Directive represent two possible avenues of development for the future of intermediary service provider liability. The AVMSD way would see the current liability immunities being upheld. Their availability would, however, be more tightly regulated and subject to more prescriptive proactive and reactive obligations along *de facto* duty-of-care responsibilities. The alternative way, pursued by the DSM Directive, would see those intermediary service providers whose activities affect the substantive law of the content or the offers in question to be primarily liable. As a result, they would fall outside the scope of the safe harbours of the ECD for this kind of violations. The risk would be that one and the same intermediary may be subject to different liability provisions – possibly for the same kind of content if that content is subject to different rights violations.

3.3.9.2. Other Rules Complementing the ECD Liability Provisions

3.3.9.2.1. InfoSoc and Enforcement Directive

Art. 8 para. 3 of the InfoSoc Directive gives rights holders the ability to apply for injunctions against intermediaries used by a third party to infringe copyright or related rights. This is supported by the IPRED, which in Art. 9 para. 1 provides for the availability of provisional and final injunctions against intermediaries as per the InfoSoc Directive. Both pieces of legislation apply without prejudice to the liability provisions of the ECD.[594] These early provisions merely supplement the ECD in that they specify the kind of sanctions that are available against intermediaries in case of intellectual property violations (cf. also above Chapter 3.3.7.3).[595]

---

594 Recital 16 InfoSoc Directive; Art. 2 para. 3 lit. a IPRED.

595 See on copyright related aspects also *Nordemann*, Liability of Online Service Providers for Copyrighted Content.

3.3.9.2.2. 2016 Guidance Note to the Unfair Commercial Practices Directive

A number of sectorial regulations have recently tried to take account of the fact that online platforms or intermediary service providers host an increasing variety of content. While the Unfair Commercial Practices Directive itself offers no link to the ECD, the Commission's 2016 Guidance note clarifies in detail the interface between obligations on online marketplaces that act as traders and the liability immunities under Art. 14 para. 1 ECD.[596]

Online platforms or marketplaces may qualify as traders according to Art. 2 lit. b of the Directive when they charge a commission on transactions between suppliers and users, offer additional paid services or derive revenue from targeted advertising. They would engage in business-to-consumer commercial practices if their actions are directly connected to promotion, sale or supply of products to consumers.[597] If a platform fulfils these conditions, and the assumption in the document is that most online marketplaces today would, they are subject to professional diligence requirements (also referred to as a standard of special skills and care) towards consumers.[598] These duties are complementary to the exemptions established under Art. 14 ECD.[599] The document cites Art. 1 para. 3 of the ECD, which states that the latter applies without prejudice to the level of protection of public health and consumer interests.[600] It therefore argues that online platforms that are considered as traders and that do not fulfil their

596 Commission staff working document, Guidance on the implementation/application of Directive 2005/29/EC, accompanying the document Communication from the Commission on a comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses, SWD/2016/0163 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0163, pp. 121–129.

597 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, pp. 22–39; Commission, Unfair Commercial Practices Directive Guidance, supra (fn. 596), p. 122.

598 Art. 2 lit. h Directive 2005/29/EC.

599 Commission, Unfair Commercial Practices Directive Guidance, supra. (fn. 596), p. 123.

600 Ibid., p. 126.

professional due diligence requirements would not be able to invoke the liability immunities of the ECD. The professional diligence requirements would consist of enabling relevant third parties to comply with EU consumer and marketing law. Examples given are "enabling relevant third party traders to clearly indicate that they act, vis-à-vis the platform users, as traders" and "designing their web-structure in a way that enables third party traders to present information to platform users in compliance with EU marketing and consumer law".[601] Unfair practices would include any misleading information provided on the characteristics of the product that influence the decision to buy[602] or omissions that the consumer needs to make an informed purchase decision.[603]

If enforced, these provisions would follow the regulatory avenue taken by the DSM Directive. Intermediary service providers acting as traders would need to meet first the professional diligence requirements of EU consumer law. This would make the protections of the ECD for online marketplaces practically obsolete.

3.3.9.2.3. Regulation on Market Surveillance and Compliance of Products

In 2017, the Commission published a notice on the market surveillance of products sold online.[604] The document noted the increasing challenges of protecting consumer health and safety posed by the rise in e-commerce and a sale of non-compliant and unsafe products. The fight against unsafe and non-compliant non-food and food products via online marketplaces is part of the Commission's horizontal strategy to tackle illegal information online.[605]

This Regulation does not provide any new responsibilities on online platforms relating to the sale of products by third party sellers. However it establishes a link between the rise in e-commerce and complex global supply chain and problems in enforcing product safety rules.[606] While uphold-

601 Ibid.
602 Art. 6 para. 1 lit. a, b and f of Directive 2005/29/EC.
603 Art. 7 of Directive 2005/29/EC.
604 Commission Notice on the market surveillance of products sold online, C/2017/5200, OJ C 250, 1.8.2017, pp. 1–19.
605 COM(2017) 555 final, supra (fn. 394), p. 3.
606 Recital 13 of Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products

ing the liability framework of Art. 12–15 ECD[607], it imposes on information society service providers an obligation to cooperate with market surveillance authorities in specific cases in order to eliminate the risks posed by products offered online.[608] It also gives market surveillance authorities powers to restrict access to "online interfaces" with non-compliant or illegal product offers.[609] An online interface is a website operated by an economic operator or on behalf of it,[610] e.g. by an online marketplace.[611]

The Regulation stops short of including information society service providers in the list of economic operators with supply chain responsibilities for product safety and consumer protection. At least the preparatory documents during the drafting phase of the Regulation show that some Member States wanted to include online platforms in the list of economic operators and asked for stronger enforcement tools against online platforms.[612] The regulation does, however, include so-called fulfilment service providers as a new type of economic operators.[613] These companies help pure e-commerce sellers to store and ship products to customers. They are enablers of e-commerce. The political will to allocate responsibilities to these new logistics platforms is a sign of how difficult it has been in the past for market surveillance authorities to enforce product safety rules within the thriving activity of online marketplaces. Many of these companies have contributed to the boom of sellers from outside the EU who market products directly to European customers.[614] It is interesting to note

---

and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169, 25.6.2019, pp. 1–44.

607 Recital 16, Art. 1 para. 4 Regulation (EU) 2019/1020 (Goods Package).

608 Art. 7 para. 2 Regulation (EU) 2019/1020 (Goods Package).

609 Recital 41, Art. 14 para. 3 lit. k point (ii) of Regulation (EU) 2019/1020 (Goods Package).

610 Art. 3 para. 15 of Regulation (EU) 2019/1020 (Goods Package).

611 For more detail: *Ullrich*, in: Maastricht Journal of European and Comparative Law 26(4), 2019, p. 558.

612 Commission Staff Working Document – Impact Assessment – Proposal for a Regulation of the European Parliament and of the Council Laying down Rules and Procedures for Compliance with and Enforcement of Union Harmonisation Legislation on Products – SWD(2017) 466 final – Part 2/4 447; *Technopolis Group*, Ex-post evaluation of the application of the market surveillance provisions of Regulation (EC) No 765/2008.

613 Art. 3 para. 11 and 13, Recital 13 of Regulation (EU) 2019/1020 (Goods Package).

614 *Ullrich*, in: Maastricht Journal of European and Comparative Law 26(4), 2019, p. 558, 570–572.

that it will be relevant to understand how in the future companies that have reduced responsibilities as an information society service reconcile this with the enhanced product compliance responsibilities they might have as fulfilment service providers.

3.3.9.2.4. Directive on Combating Terrorism

The Directive (EU) 2017/541 on combating terrorism has a special provision that requires Member States to ensure the prompt removal of any online (and offline) content that constitutes a terrorist offence.[615] The Directive states that any efforts to remove or block access to content which constitutes a terrorist offence should be without prejudice to the ECD. It repeats the prohibitions to require service providers to generally monitor information or proactively seek facts that would indicate illegal activity (Art. 15 para. 1 ECD). It also repeats the hosting service immunities established in Art. 14 para. 1 lit. a ECD which relate to a lack of knowledge.[616] This Directive has a purely complementary and clarifying character with regard to the remedies available against intermediary service providers in the fight against terrorist content online.

3.3.9.2.5. Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online

The Commission proposed this Regulation in September 2018 in order to tackle the threat of terrorist content online (cf. more detailed above Chapter 2.4.5.2). The proposal is targeted specifically at hosting service providers in order to mitigate the use of their service for spreading terrorist offences.[617] It is currently in the EU legislative process and it will need to be seen how it evolves during the mandate of the new Commission when

615 Art. 3 para. 1 lit. a and Art. 5 of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, pp. 6–21.

616 Ibid., Recital 23.

617 Cf. on the relationship between the proposal and the ECD also *Barata*, New EU Proposal on the Prevention of Terrorist Content Online – An Important Mutation of the E-Commerce Intermediaries' Regime.

trilogue negotiations potentially will start. Its initially proposed text[618] has been significantly amended by the European Parliament. This analysis will focus on the latest version of the text[619] where it concerns the liability provisions of the ECD.

It should be noted that the proposal focusses on the *prevention* of the dissemination of terrorist content through hosting providers. It therefore touches on the core of the debate on what intermediary service providers can be asked to do proactively without losing their immunities. The Parliament amendment upholds and reaffirms the protections of the ECD immunities for intermediary service providers, where the Commission's proposal had originally sought to mandate broader proactive measures for hosting providers.[620] In particular a controversial exception that would for the first time have given the authorities the option to override the prohibition to impose general monitoring duties on hosts (Art. 15 ECD) has been deleted.[621] Meanwhile a passage that obliges hosting providers to act with duty of care regarding the prevention of terrorist content has remained in, although in significantly changed form.[622] The duty of care consists of hosting providers protecting users in a "diligent, proportionate and non-discriminatory manner" from terrorist content, while upholding the provisions of Art. 14 and 15 ECD. In addition, it now provides a useful reference to the revised AVMSD by stating that video-sharing service providers would be bound by Art. 28b of that Directive.[623]

Art. 6, originally named "proactive measures", is now called "specific measures". In fact, any of the 33 references to proactive measures in the Commission's proposal has been either deleted or replaced by the Parliament. Since the proposal is aimed at the prevention of terrorist content, this might have been considered redundant. However, as becomes clear through the amended version of Art. 6, one of the main objectives of the Parliament was to ensure that hosting providers would not be incited to engage in unduly broad preventive monitoring activities that could lead to conflict with Art. 15 para. 1 ECD. For example, the amended proposal now

618 COM/2018/640, supra. (fn. 369).
619 European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online TA/2019/0421, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=EP:P8_TA(2019)0421.
620 Ibid., Recital 9.
621 Ibid., Recital 9.
622 Ibid., Art. 3.
623 Ibid., Art. 3 para. 2b.

allows Member States to ask those hosting providers who had received a substantial number of removal orders from authorities to put in place specific measures. These measures must not impose a general monitoring obligation or the use of automated tools.[624] Nevertheless, the fact that hosting providers still need to weigh the use of specific measures "in light of the risk and level of exposure to terrorist content" and of fundamental rights means that they are asked to engage in an *ex ante* risk assessment and balancing exercise which is characteristic of a duty of care.[625]

The proposal also obliges hosting providers to issue transparency reports on any removals and the use of automated tools. The Parliament has amended these obligations by requiring hosting providers to include more detail and data than original proposed by the Commission.[626] Again reporting obligations are an essential part of a duty of care. Art. 9–11 establish additional duties on hosting providers on content that has been taken down. These are: mechanisms on the adequacy and proportionality of automated tools, effective complaints, counter claim and information procedures for removed content.

As the proposal stands now – and, as mentioned, this is only the Parliament's position which will be subject to compromise negotiations once the Council has concluded a General Approach –, it already formalises, substantiates and steps up procedures that hosting services will need to comply with in the fight against illegal terrorist content in order to avail themselves of the immunities offered under the ECD. It therefore follows the route taken in the new AVMSD.

3.3.9.2.6. General Data Protection Regulation

The GDPR does not contain any specific provisions that regulate the activities of Internet intermediaries. It merely mentions that it does apply without prejudice to the ECD, in particular with the liability rules of intermediaries in Art. 12–15 ECD.[627] This suggests that the GDPR and ECD are to be considered as complementary. The practical consequences of this ar-

624 Ibid., Art. 6 para. 4.
625 Ibid., Art. 6 para. 1.
626 Ibid., Art. 8.
627 Recital 21, Art. 2 para. 4 GDPR, supra (fn. 20); cf. on the relationship between GDPR and ECD also *de Gregorio*, The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?

rangement are, however, far from clear due to open language in both acts. The ECD itself states in Art. 1 para. 5 lit. b that it "shall not apply to questions relating to information society services covered by Directives 95/46/EC and 97/66/EC" (the data protection and privacy in telecommunication rules at the time: cf. in detail already Chapter 2.4.3). Suffice to state here that so far conflicts between data protection and intermediary liability rules have only developed gradually. On a conceptual level, one could argue that both provisions barely touch one another.[628] The GDPR is about the protection of privacy of data subjects. However, Internet intermediaries are involved also with considering data protection aspects when they action "right-to-be-forgotten" requests or notice-and-takedown or information requests from authorities. But these activities concern the actions of the intermediary in the course of exercising its obligations under content liability rules. Whether the intermediary executes these obligations in compliance with GDPR or not does not change the extent of the liability over the third-party content itself.

The case may be different where the breach of data and privacy protection rules are at the heart of content uploaded by a user, such as the right-to-be-forgotten or videos depicting persons that did not consent to being shown. If an intermediary was notified of this and failed to act, then the infringing activity would relate to breaches of data protection rules and the intermediary could be held (primarily) liable for that.[629] The CJEU attempted to outline that delineation in the *Google Spain* ruling.[630]

3.3.9.2.7. Platform-to-Business Regulation

The EU passed the Regulation promoting fairness for business users of online intermediation services[631] in June 2019 to address the problem of imbalances in bargaining power in the interactions between business users and online platforms.[632] The Regulation targets e-commerce market places, including collaborative platforms, app stores, social media services

628 For a detailed discussion of the interplay between the ECD's intermediary liability rules and the GDPR see: *Keller*, in: Berkeley Technology Law Journal 33(1), 2018, p. 287, 354.
629 Ibid., p. 359.
630 CJEU, *Google Spain v AEPD*, supra (fn. 79), para. 38
631 Regulation (EU) 2019/1150, supra (fn. 364).
632 Ibid., Recital 2.

and online search engines (cf. already Chapter 2.4.5.1 in detail).[633] While no reference exists to the ECD, the regulation clearly identifies these services as information society service providers according to Directive 2015/1535.[634] Although restricted to commercial users of platforms, the regulation makes provisions that can be of interest in the debate over the liability immunities for hosting providers under the ECD. Search engines, for example, will need to disclose the parameters used for ranking results and provide detail on any possibilities that exist for users to influence rankings.[635]

Other online intermediation services need to disclose differential treatment given to those users which they control directly.[636] This would include details on access given to data for users which are controlled by the intermediation service, internal pricing information relating to rankings, setting or technical services or functionalities.[637] Furthermore, online intermediation services need to give business users details on what access they have to general and personal data provided by the user or generated by the user on the platform.[638] The transfer of data through third parties also needs to be disclosed and the purpose explained, with the possibility for the business user to opt out from this activity.[639]

The motivations for this Regulation and its provisions really throw further doubt on the adequacy and timeliness of the current liability immunities of the ECD, which rest on the mere technical, automatic and passive nature of the activities of intermediary service providers. It can be argued that any online intermediation service provider that would, under this Regulation, disclose differential treatment and far-reaching accesses to, and

633 Ibid., Recitals 6, 11, Art. 1 para. 2.
634 Ibid., Art. 2 para. 2 lit. a; Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, pp. 1–15.
635 Regulation (EU) 2019/1150, supra (fn. 364), Art. 5.
636 Ibid., Art. 7. A typical example would be differences in display or ranking of a product sold by Amazon as opposed to the same product sold on the Amazon marketplace by a third party seller. Cf. Commission, press release of 17.7.2019, Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_19_4291.
637 Art. 7 of Regulation (EU) 2019/1150, supra (fn. 364).
638 Ibid., Art. 9.
639 Ibid., Art. 9 para. 2 lit. d.

exploitation of, user data[640] can hardly claim to be a passive host under the ECD. A future Digital Services Act by the EU should take note of this Regulation when redrafting the liability conditions for intermediary service providers.

640 Which is part of the business model of Web 2.0 platforms.