Liability exemptions of non-hosting intermediaries: Sideshow in the Digital Services Act?

Schwemer, Sebastian Felix; Mahler, Tobias; Styri, Håkon

Published in:
Oslo Law Review

DOI:
https://doi.org/10.18261/ISSN.2387-3299-2021-01-01

Publication date:
2021

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

Oslo Law Review

SCANDINAVIAN UNIVERSITY PRESS

RESEARCH PUBLICATION

Volume 8, No. 1-2021, p. 4–29
ISSN online: 10.18261/ISSN.2387-3299
DOI: https://doi.org/10.18261/ISSN.2387-3299-2021-01-01

Liability exemptions of non-hosting intermediaries: Sideshow in the Digital Services Act?

Sebastian Felix Schwemer
Associate Professor, Centre for Information and Innovation Law (CIIR), University of Copenhagen
Adjunct Associate Professor, Norwegian Research Center for Computers and Law (NRCCL), University of Oslo
sebastian.felix.schwemer@jur.ku.dk

Tobias Mahler
Professor, Norwegian Research Center for Computers and Law (NRCCL), University of Oslo
tobias.mahler@jus.uio.no

Håkon Styri
Senior Advisor, Norwegian National Security Authority

Abstract
The European Union is currently discussing a reform of its intermediary liability rules with its recently proposed Digital Services Act. The existing rules in the e-Commerce Directive (Directive 2000/31/EC) offer a safe harbour from liability for certain intermediary functions that are central to the functioning of the internet. A safe harbour for intermediaries is one of the regulatory cornerstones that help protect innovation, creativity and the free flow of information. At the same time, these rules are under pressure. This paper discusses a subset of 'non-hosting' intermediary functions. Some of these have traditionally been less visible in content-related regulatory debates. We look at selected examples of functions related to the domain name system (DNS), content delivery networks (CDNs), cloud processing and live-streaming. The current liability exemption regime under the e-Commerce Directive focusses on transmission in, or access to, a communication network, as well as storage. However, significant grey areas arise both in relation to what we call the 'auxiliary network intermediary' function (as opposed to 'direct network intermediary' functions corresponding to 'mere conduit' functions), which does not transmit or provide access, and the 'temporal provision and processing of information', which is different from storage.

Keywords
Intermediary liability, self-regulation, content regulation, Digital Services Act, e-Commerce Directive, content delivery networks, domain name system

1. Introduction

The European Union (EU) is currently discussing a reform of its intermediary liability exemption rules. With a view to updating these rules, the European Commission presented on 15 December 2020 its proposal for a Regulation, termed the Digital Services Act (DSA).[1] The existing rules in the e-Commerce Directive (ECD)[2] offer a safe harbour from liability for certain intermediaries (or rather specific functions), which are central to the operations of the internet. A safe harbour for intermediaries is one of the regulatory cornerstones that help protect innovation, creativity and the free flow of information—as emphasised, for example, in the NETmundial Principles.[3] As opposed to, for example, US safe harbour protections of intermediaries,[4] the European rules apply horizontally, with a single set of rules that cover all forms of liability, including civil and criminal liability, for all forms of information content.[5] At the same time, these rules are under pressure as lawmakers, interest groups and society at large scrutinise the future role of intermediaries. This paper discusses a subset of intermediaries, which can broadly be called 'non-hosting' intermediaries. We address selected examples of functions related to the domain name system (DNS), Wi-Fi hotspots, content delivery networks (CDNs), cloud processing, and search engines. Traditionally, these intermediary functions have been less visible in content-related regulatory debates, but they have recently gained more salience.

In ongoing content moderation and regulation debates, both in Europe and abroad, much focus is (rightly) on the role of (gatekeeper) platforms.[6] One example is the recent debate about the liability of online platforms for user-uploaded copyright-protected content.[7] With this paper, we want to contribute to this discourse in the legal and the internet governance scholarly communities and nuance it with a perspective on the role of 'non-hosting' intermediaries in content regulation. Conceptually, intermediaries at the infra-

1. Commission, 'Proposal for a Regulation of the Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC', COM/2020/825 final. See also eg Commission, 'Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services' (Combined Evaluation Roadmap/Inception Impact Assessment) Ares(2020)2877686.
2. Directive of the European Parliament and of the Council 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L 178/1.
3. See Global Multistakeholder Meeting on the Future of Internet Governance, 'NETmundial Multistakeholder Statement' (24 April 2014) <https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf> accessed 10 March 2021. These non-binding principles are the outcome of a two-day global meeting that joined governments, global internet organizations, civil society and scholars to discuss a governance roadmap for the internet.
4. See Communications Decency Act of 1996 ('CDA'), Pub L No 104-104 (Tit V), 110 Stat 133 (8 February 1996), codified at 47 USC § 230; and Digital Millennium Copyright Act, ('DMCA'), Pub L No 105-304, 112 Stat 2860 (28 October 1998), codified at 17 USC 512, 1201-05, 1301-22; 28 USC 4001 § 512.
5. Notice, however, the recent carving out for certain online content-sharing service providers, such as YouTube, in Art 17 of Directive of the European Parliament and of the Council 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92 ('CDSM Directive').
6. See eg Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online [2018] OJ L 63/50; Article 17 CDSM Directive; national secondary legislation—eg in France (*Loi n° 2019-775 du 24 juillet 2019 tendant à créer un droit voisin au profit des agences de presse et des éditeurs de presse*).
7. See eg Martin Husovec and João Quintais, 'How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms' (2020) 4 *GRUR International* (forthcoming) <http://dx.doi.org/10.2139/ssrn.3463011>; Sebastian F Schwemer, 'Article 17 at the Intersection of EU Copyright Law and Platform Regulation' (2020) 3/2020 *Nordic Intellectual Property Law Review* 399; Thomas Riis and Sebastian F Schwemer, 'Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation' (2019) 22(7) *Journal of Internet Law* 1 <http://dx.doi.org/10.2139/ssrn.3300159>.

structure or logical layer of the internet are much further away from content compared with their hosting and platform counterparts. Yet, we observe a shift in the narrative around these non-hosting intermediaries. Certain domain registries, for example, have—voluntarily—put in place notice-and-action regimes akin to platforms, partly going beyond the technical abuse of infrastructure and addressing content abuse. Another example of this shift relates to content delivery networks (CDNs), which have been taken to court by intellectual property rights holders both in Europe and the US to test their liability exemption.

Our starting point is the liability exemption regime of the EU's ECD, which celebrated its 20th birthday on 8 June 2020. The conditions for benefitting from a liability exemption have, in practice, led to such arrangements as notice-and-action models in relation to online platforms under Article 14 ECD. Outside of hosting, the ECD's rules traditionally address internet access service providers (Article 12), which are well described in the academic literature, and proxy caching (Article 13). However, in the 21 years since the adoption of the Directive, internet technology has developed, and it is possible that the safe harbour was defined too inflexibly from the start. This issue is especially topical because the proposed DSA is about to cement the existing safe harbours from the Directive in a Regulation.[8] As noted, instead of providing an in-depth analysis of the proposed rules, we take our starting point in the existing framework of the ECD and test to what extent certain old and new functions other than hosting qualify under the safe harbours, and with what likelihood.

2. Non-hosting internet intermediaries: between transnational private regulation and EU law

2.1 The regulatory landscape

According to the Organisation for Economic Co-operation and Development (OECD), 'Internet intermediaries bring together or facilitate transactions between third parties on the Internet'.[9] The OECD's definition goes on to mention the many different intermediary functions, such as 'to give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties'. In EU legislation, there exists no corresponding intermediary definition, and the notion of non-hosting intermediary is not used in EU legislation[10] or technical protocols.

Protocols constitute a layer of transnational private regulation as soft law, which complements national and regional regulation (eg EU law). This transnational de facto regulation, even if only soft law, has a strong influence on the architecture and functioning of the internet. Accordingly, the Internet Engineering Task Force (IETF) describes the internet as 'a loosely-organized international collaboration of autonomous, interconnected networks,

8. The wording of the liability exemptions for 'mere conduit', 'caching' and hosting remain largely unchanged in the Commission's proposal for the DSA.
9. Karine Perset, 'The Economic and Social Role of Internet Intermediaries' (2010) No 171 *OECD Publishing* 9 <https://doi.org/10.1787/5kmh79zzs8vb-en> accessed 10 March 2021.
10. See the discussion below on 'information society service provider'. In the context of due diligence obligations, the DSA ('Chapter III Due diligence obligations for a transparent and safe online environment') proposes to introduce the novel notion of an 'intermediary service' in Article 2(f), which differentiates between 'mere conduit', 'caching' and 'hosting' services.

[which] supports communication through voluntary adherence to open protocols and procedures defined by Internet Standards'.[11] The technical standards and other documentation that are used to make the internet work are published by the IETF, which is a large open international community of network designers, operators, vendors and researchers.[12] The standards are open and created by a procedural commitment to 'rough consensus and running code'.[13] Standards from other organisations, for example, the World Wide Web Consortium (W3C), are used for the wide variety of services that use the internet, and proprietary standards are relied on to create new services too. Regarding open standards, the principle of rough consensus and running code implies that software vendors, such as browser developers, are in a strong position when new standards are created. Further examples related to the DNS and Internet Protocol (IP) addresses are the Internet Corporation for Assigned Names and Numbers (ICANN),[14] the Internet Assigned Numbers Authority (IANA),[15] and the Reseaux IP Europeens Network Coordination Centre (RIPE NCC).[16] Open standards are also sometimes established outside these organised settings by private companies.[17] This de facto regulation accompanies legislation related to intermediaries. Without a liability exemption, intermediaries could risk liability for illegal content communicated with their direct or indirect help. For example, an internet access provider (IAP) forwarding internet traffic could potentially be held liable if that traffic included illegal material. In Europe, the liability exemption of online intermediaries is harmonised by the ECD.

The ECD is a relatively technology-neutral regulation, because the functions performed by intermediaries are described in general terms, such as 'transmission in a communication network of information'.[18] At the same time, this neutrality is limited because the ECD conceptualises intermediary functions based on a particular architecture: it defines the liability exemptions based on certain specific functions, namely, 'mere conduit'[19] (Article 12 ECD), 'caching'[20] (Article 13 ECD) and hosting (Article 14 ECD).

In some instances, the regulation of intermediaries is also influenced by other EU legislation, and certain functions may be regulated by several frameworks, addressing such issues as competition and consumer protection in electronic communications networks,[21]

11. IETF, 'Internet standards' <www.ietf.org/standards/> accessed 9 March 2021.
12. Harald Alvestrand and Håkon Wium Lie, 'Development of Core Internet Standards: The Work of IETF and W3C' in Lee A Bygrave and Jon Bing (eds), *Internet Governance: Infrastructure and Institutions* (Oxford University Press 2009) 126-46.
13. On the historical dimension of this statement, see eg Andrew L Russell, '"Rough Consensus and Running Code" and the Internet-OSI Standards War' (2006) 28(3) *IEEE Annals of the History of Computing* 48-61 <https://doi.org/10.1109/mahc.2006.42>.
14. An internationally organised, non-profit corporation, ICANN is responsible for allocating Internet Protocols (IP), assigning protocol identifiers and management of the generic Top-Level Domain (gTLD) and country code Top-Level Domain (ccTLD) name system, as well as the root server system; see 'Welcome to ICANN!' (ICANN) <www.icann.org/resources/pages/welcome-2012-02-25-en> accessed 10 March 2021.
15. IANA is a standards organisation with functions that have historically included 'the maintenance of the registry of technical Internet protocol parameters; the administration of certain responsibilities associated with Internet DNS root zone and the allocation of Internet numbering resources' (see ibid).
16. RIPE NCC is a non-profit organisation responsible for the allocation and registry of internet number resources; see 'What We Do' (RIPE NCC, 19 June 2020) <www.ripe.net/about-us/what-we-do> accessed 12 March 2021.
17. For example, the Google AMP framework.
18. See Article 12 ECD.
19. Note the quotation marks in the legal text.
20. Note the quotation marks in the legal text.
21. Directive of the European Parliament and of the Council 2018/1972 establishing the European Electronic Communications Code [2018] OJ L 321/36.

network neutrality,[22] cybersecurity,[23] data privacy[24] or audio-visual media on the internet.[25] There may also be sector-specific national legislation, such as in relation to illegal content,[26] but this issue is not explored further in this article.

Furthermore, related to but separate from the question of liability is the role of injunctions. Importantly, the liability exemptions in the ECD merely shield from liability; they do not restrict a court or administrative authority to issue an injunction with a view to require the service provider to terminate or prevent an infringement in accordance with the national legal system in the respective Member State (MS).[27] Injunctions are of major practical importance and there exists ample case law regarding injunctions, most notably in relation to internet access service providers; however, discussion of these issues is outside the scope of this article.[28]

---

22. Regulation (EU) of the European Parliament and of the Council 2015/2120 of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union [2015] OJ L 310/1. It restricts, for example, IAPs from certain traffic management measures, including voluntary content blocking without legal basis.
23. For example, digital infrastructure (IXPs, DNS service providers, TLD name registries) in the Directive of the European Parliament and of the Council 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1 ('NIS Directive'). However, the intersection with the ECD is not explored in the Commission, 'Annex to Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', COM(2017) 476 final/2, see 36 ff, which indicates that a conflicting overlap was not identified between the two frameworks.
24. Regulation (EU) of the European Parliament and of the Council 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2018] OJ L 119/1 (GDPR). For example, the right to erasure in Article 17 GDPR may be relevant. In October 2020, the European Commission proposed an interim Regulation containing derogations from the ePrivacy Directive's provision (Directive of the European Parliament and of the Council 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications [2002] OJ L 201/37) concerning confidentiality of communication and traffic data in light of the entry-into-force of the European Communications Code in December 2020. The derogation concerns the practice of voluntary measures to tackle child sexual abuse material (CSAM) by number-independent interpersonal communications service providers, such as Voice over IP, messaging and web-based e-mail services (including Facebook Messenger and similar). See eg Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online', COM(2020) 568 final.
25. Directive of the European Parliament and of the Council 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services ('Audiovisual Media Services Directive') [2010] OJ L 95/1, as amended by Directive (EU) of the European Parliament and of the Council 2018/1808 of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L 303/ 69 ('AVMSD').
26. For example, online gambling, which is excluded from the ECD's scope according to Article 1(5)(d)(4) ECD. See Commission, 'Online gambling in the Internal Market, Accompanying the document Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions Towards a comprehensive framework for online gambling', SWD/2012/0345 final.
27. See Articles 12(2) and 13(2) ECD in the same wording; see also Recital 45. Article 14 ECD (hosting), in addition to injunctions, furthermore stipulates that the liability exemption 'does [not] affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information'.
28. See eg Martin Husovec, *Injunctions Against Intermediaries in the European Union. Accountable but not liable?* (Cambridge University Press 2017); Gerald Spindler, 'Responsibility and Liability of Internet Intermediaries: Status Quo in the EU and Potential Reforms' in Tatiana E Synodinou and others (eds), *EU Internet Law* (Springer 2017) ch 12 <https://doi.org.10.1007/978-3-319-64955-9_12, 289-314>.

2.2 What are 'non-hosting' functions?

This article focusses on liability exemptions for 'non-hosting' functions of intermediaries. To explain our distinction between hosting and non-hosting, it is necessary to understand the design of European liability exemption rules. We employ a broad understanding of 'non-hosting'. We simply use this as a categorisation of services *other* than hosting (akin to the legal delimitation in Article 14 ECD). In the EU context, hosting refers to services where content provided by the recipient of a service is traditionally stored for a prolonged period. An example of such a hosting function relates to (some of) the services offered, for example, by such online platforms as YouTube, Facebook or Twitter. However, note that hosting as a technical concept[29] does not necessarily imply that content is stored.

Compared with the liability exemption for hosting functions (Art 14 ECD), the intermediary functions of the two remaining liability exemptions ('mere conduit' and 'caching', Articles 12 and 13 ECD) have been less prominently featured in recent policy discussions at the European and national levels.[30] There exist many technical and legal differences between hosting (read: platforms) on the one hand and 'mere conduit' and 'caching' on the other. For example, hosting providers can take down content if notified of its illegality. By comparison, an internet access provider—or other non-hosting provider (discussed below)—may not be in a position to take down content. The actions available for non-hosting providers are often limited, and many content-related measures can easily lead to over-blocking. These differences are important to understand with a view to avoiding unintended spill-over effects from regulatory efforts regarding hosting, ie measures that may make sense in the context of intermediaries broadly related to platforms but not in the non-hosting intermediary landscape. Within non-hosting, we do not focus on the provision of internet access but on various other grey areas, which are less explored in the academic literature.[31] Examples include DNS and Wi-Fi services, cloud processing and content delivery networks (CDNs). These functions raise a number of specific regulatory problems that are easily put in the shadow of internet access service providers on the one hand and hosting providers on the other.

At a fundamental level, the non-hosting notion can be seen as a collection of legal concepts. In legal texts, the complexity of the world often needs to be condensed into legal concepts, which complement rights and obligations. These legal concepts are not 'norms of conduct' because they do not directly regulate what actions are obligatory or permitted. However, whether a right or obligation applies in practice depends on whether its conditions are fulfilled, and this is where legal concepts play a role in the logic of the law.[32] Intermedi-

29. The technical term 'host' covers any computer or similar device connected to a computer network.
30. Given the prominent role of online platforms (which often but not always are considered hosting services) in today's internet landscape, this focus seems understandable. See eg Commission, 'Online Platforms and the Digital Single Market – Opportunities and Challenges for Europe', COM(2016) 288 final; Commission, 'Communication on Tackling Illegal Content Online – Towards an enhanced responsibility of online platforms', COM(2017) 555 final; Commission Recommendation (EU) 2018/334 (n 6); the copyright-specific carveout of Article 14 ECD in Article 17 CDSM Directive.
31. The selection of non-hosting functions is based on the authors' study for the Commission, where the Commission indicated these specific non-hosting functions of interest when drafting the DSA.
32. Legal logic not only includes deontic notions (eg obligation, prohibition, etc) but also operates with constitutive rules, or 'counts as' connections, in the form of 'x counts as y'. For example, if certain defining characteristics are fulfilled, a service may qualify, or count as, hosting. See generally Giovanni Sartor, *Legal Reasoning: A Cognitive Approach to Law* (Springer 2005) 551ff. The terminology for these types of norms differs. Some call these '*constitutive*' norms (see eg Alf Ross, *Directives and Norms*, International Library of Philosophy and Scientific Method (Routledge & Kegan Paul 1968) 54ff); others prefer to call these norms 'determinative' (as used by Georg Henrik von Wright, *Norm and Action: A Logical Enquiry* (Routledge & Kegan Paul 1963) 6ff); yet others prefer '*conceptual*' norm (see Eugenio Bulygin, 'On Norms of Competence' (1992) 11(3) *Law and Philosophy* 210ff) or '*quali-*

ary liability is a case in point. Certain functions are exempted from liability if they fulfil the requirements (conditions) of the law, which attempt to capture key aspects of the complex way in which internet communication works. These requirements (for liability exemption) are different from the rules under EU MS law, according to which actors can be held liable. Ultimately, the decision about liability in a concrete case must consider both liability rules and conditions for exemptions. The spectrum of non-hosting services is heterogeneous as it covers a wide range of offerings. These have in common that they, as intermediaries, bring together or facilitate transactions between third parties on the internet.

2.3 Conditions for liability exemptions in the EU framework

The ECD's horizontal liability exemption regime (ie covering administrative, civil and criminal liability) comes with two general criteria that need to be fulfilled: first, the service provider needs to provide a specific form of an 'intermediary' information society service, and second, that information society service provider's (ISSP's) activity must qualify as passive. The specific liability exemptions for the three types of intermediary activities then come with certain—graduated—conditions that need to be fulfilled.[33] Importantly, it is only the three functions of 'mere conduit' (Article 12 ECD), 'caching' (Article 13 ECD) and hosting (Article 14 ECD) that are exempt from liability.

The ECD does not address (internet) intermediaries[34] as such; rather, it focusses on the broad,[35] EU-specific genus of the ISSP, which is defined as an autonomous concept in Article 1(1)(b) of the Technical Standards Directive.[36] According to this definition, such a service first needs to be 'normally provided for remuneration'. This criterion is of special interest in the non-hosting sphere, where the service is sometimes not paid for by the beneficiary of the service, and it may be unclear who the recipient of various services is (eg registrant paying for the domain name to be accessible or proxy caching being paid for by internet access service providers (IAPs)). Already, in accordance with the Court of Justice of the European Union's (CJEU's) case law,[37] Recital 18 ECD clarifies that

> 'information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information

fictional' norm (see Nils Kristian Sundby, *Om Normer* (Universitetsforlaget 1974) 77ff). By comparison, Hart distinguishes between primary and *secondary* rules: see H L A Hart, *The Concept of Law* (2nd ed, Clarendon Press 1961; repr 1994) 94.

33. Also compare the Commission's proposal for the ECD: 'The distinction as regards liability is not based on different categories of operators but on the specific types of activities undertaken by operators'. See Commission, 'Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market', COM(1998) 586 final 27.
34. Despite Section 4 of the ECD (Articles 12–15) addressing intermediary service providers and the commonplace usage of 'intermediary' in practice and academia, the notion 'intermediary' is not further specified in the ECD and needs to be distinguished from the ISSP notion.
35. See also Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 388.
36. See Article 2(b) ECD and Article 1(1)(b) of Directive (EU) of the European Parliament and of the Council 2015/1535 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 [2015] OJ L 241/1 ('Technical Standards Directive').
37. Case 352/95, *Bond van Adverteerders and others v The Netherlands State*, judgment of 26 April 1988 (ECLI:EU:C:1988:196) para 16. See also Case C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH*, judgment of 15 September 2016 (ECLI:EU:C:2016:689) para 43.

via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service'.

Thus, whereas the service must represent an economic activity, a broad interpretation must be given, and it does not require the service to be paid for directly by those for whom it is performed.[38] The service also needs to be provided at a distance, which does not appear to have created issues so far in case law. Furthermore, the definition only covers a service provided by electronic means, which also appears to be unproblematic in the current technological remit.[39] The definitions in the ECD and the Technical Standards Directive can be seen as technologically neutral, in the sense that they do not refer to the internet, which is based on the Transfer Control Protocol (TCP)/IP suite. Thus, other potentially evolving forms that might replace TCP/IP could also be encompassed by the rules. Finally, such a service needs to be at the individual request of a recipient. This criterion does not appear to have given rise to concerns but might challenge the applicability of the ECD in relation to some services (eg live-streaming).

According to Recital 42 ECD, as a second prerequisite, 'this activity is of a mere technical, automatic and passive nature, which implies that the ISSP has neither knowledge of nor control over the information which is transmitted or stored'.[40] In *McFadden*, the CJEU stipulated in relation to 'mere conduit', for example, that 'providing access to a communication network must not go beyond the boundaries of such a technical, automatic and passive process for the transmission of the required information',[41] without providing further guidance on the criterion. Thus, on the flipside, an 'active' service provider cannot benefit from the liability exemptions in the ECD. The distinction between active and passive is not as clear as it seems, as the situation both conceptually and technically is regularly more nuanced than

38. See *McFadden* (n 37) Opinion of AG Szpunar delivered on 16 March 2016 (ECLI:EU:C:2016:170) paras 37-38. See also C-291/13, *Sotiris Papasavvas v O Fileleftheros Dimosia Etaireia Ltd and Others*, judgement of 11 September 2014 (ECLI:EU:C:2014:2209) paras 4 and 29. Regarding internet search engine service providers, 'who do not provide their service in return for remuneration from the internet users', AG Jääskinnen in the *Google Spain* case, for example, surprisingly argued for an analogous application based on the assessment that such providers 'appear to fall in that capacity outside the scope' of the ECD: see Case C-131/12, *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Opinion of AG Jääskinen delivered on 25 June 2013 (ECLI:EU:C:2013:424) para 37. This is contrary to the broad interpretation and was not picked up by the CJEU. Yet, it illustrates that the economic requirement of the ISSP definition may be challenging to apply.

39. 'Electronic means' is regularly used as a short form of 'electromagnetic means' and includes optical means. In theory, there may be technological developments outside the 'electromagnetic' realm based on quantum theory, but this is unlikely to happen within a reasonable regulatory timeframe.

40. The criterion of passivity has explicitly formed part of the Directive in relation to Articles 12 and 13 ECD. See Case C-521/17, *Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta* judgment of 7 August 2018 (ECLI:EU:C:2018:639) para 47; *McFadden* (n 37) para 62. In the context of hosting applied by the CJEU, see Case C-324/09, *L'Oréal SA and Others v eBay International AG and Others*, judgment of 12 July 2011 (Grand Chamber) (ECLI:EU:C:2011:474) para 113; Joined Cases C-236/08 to C-238/08, *Google France SARL and Google Inc v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08)*, judgment of 23 March 2010 (Grand Chamber) (ECLI:EU:C:2010:159) para 113; *Papasavvas* (n 38), para 40 ff. However, this is not uncontested: see eg Case C-324/09, *L'Oréal SA and Others v eBay International AG and Others*, Opinion of Advocate General Jääskinen delivered on 9 December 2010 (ECLI:EU:C:2010:757) paras 138-42; Riordan (n 35) 402; Sophie Stalla-Bourdillon, 'Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the e-Commerce Directive as Well' in Luciano Floridi and Mariarosaria Taddeo (eds), *The Responsibilities of Online Service Providers* (Springer 2016) 13; Annemarie Bridy, 'The Price of Closing the "Value Gap": How the Music Industry Hacked EU Copyright Reform' (2020) 22(2) *Vanderbilt Journal of Entertainment & Technology Law* 323 <https://dx.doi.org/10.2139/ssrn.3412249>.

41. *McFadden* (n 37) para 46.

'just active' or 'just passive'.[42] The active/passive dichotomy is increasingly challenging to apply in practice because it is in the nature of a service that it involves some degree of activity.[43] Thus, the provider is active in some respects and passive in others. However, a closer reading of the above-mentioned recital shows that the ultimately decisive factors should be knowledge and control over the information. Further clarifications might be needed.

Questions arise, especially when an intermediary offers functions in combination with hosting. These could be seen as separate services or functions, with the consequence that some are covered by a liability exemption while related functions may not be. The intermediary could then still be held liable for the non-exempted function but not for hosting. In a sense, such related functions could be considered non-hosting, and the question arises of whether there would exist good arguments for exempting them. Alternatively, the combined service, consisting of several functions, could also be seen as a unity. In that case, the question arises of whether the related function could be of such character that it voids the passivity requirement with the consequence that the service qualifies as active and falls outside the scope of application of the liability exemption.[44] Alternatively, we may ask whether the combined service would deserve an exemption *de lege ferenda*.

2.4 Considerations *de lege ferenda*

When going forward with an update of intermediary liability rules, the European lawmaker needs to strike a fair balance between the various stakeholder interests, emphasising fundamental rights.[45] Both risk management and proportionality are relevant reference points for an updated framework. There is a trade-off between mitigating content risks and ensuring that measures against illegal content remain proportional.

The communication of illegal content or information implies a risk to some stakeholders' rights and interests. For example, children are at risk when child sexual abuse material (CSAM) is produced and disseminated. Economic literature emphasises that risk should be allocated to the actor who is best suited to avoid it,[46] and intermediaries can influence the communication of illicit content. However, the context of intermediary liability is complex and involves a variety of actors and stakeholders, so a simple risk allocation is unfeasible. Intermediary service providers differ in their ability to manage content risks, partly because they vary in their proximity to the illegal content. This parameter (proximity to unlawful content) could play a role in allocating risk. Arguments for liability could include near business relations with the originator of illicit content or a close technical connection to the material.[47] Based on a simple risk allocation rationale, intermediaries with proximity to illegal content risk should bear these risks. However, such a risk assignment would also create incentives for mitigating risks by taking down content, which is not without consequences.

---

42. See also Joris van Hoboken and others, *Hosting Intermediary Services and Illegal Content Online, A Study Prepared for the European Commission* (DG Communications Networks, Content & Technology, SMART number 2018/0033, 2020) 31-36. Recital 18 DSA proposal puts emphasis on the 'neutral' provision of services.
43. In the future, the 'automatic' criterion, which could be understood as relating to a rule-based system, might also be challenged by developments in the field of machine learning and artificial intelligence, which are not necessarily rule based.
44. See eg *L'Oréal and Others* (n 40).
45. See eg *McFadden* (n 37) paras 83, 98.
46. See eg Sai On Cheung, 'Dispute Avoidance Through Equitable Risk Allocation' in Sai On Cheung (ed), *Construction Dispute Research Conceptualisation, Avoidance and Resolution* (Springer 2014) 99.
47. See Sebastian F Schwemer, Tobias Mahler, Håkon Styri, *Legal Analysis of the Intermediary Service Providers of Non-Hosting Nature,* Final report prepared for European Commission (2020) 40-43.

The key problem is that taking down content also affects other stakeholders, such as internet users and society at large. Therefore, fundamental rights ought to constitute an essential starting point for the liability exemption framework. The lawmaker should weigh benefits (the protection from impacts of unlawful content) against costs (the negative effects of protection measures on other fundamental rights). Intermediaries are exempted from liability because they fulfil important societal functions. Their roles in the communications process structurally limit their ability to take proportionate and effective measures to control content-related risks without negative effects on an open and free internet. This is also acknowledged in the case law of the CJEU, which points out that one needs to strike a fair balance between the rights and interests at stake.[48] Measures imposed on a service provider must balance these rights and be proportionate.

In the non-hosting context, the various service providers differ significantly in their ability to take measures that could potentially affect content-related risks. Therefore, we must ask what technical measures the respective service providers possess and how these affect fundamental rights. Such measures include the taking down of infringing material for hosting providers, but non-hosting service providers typically cannot take down content. Non-hosting providers can influence the availability of content (eg through website blocking), but such options' effectiveness and precision are critical for avoiding disproportionately detrimental effects on fundamental rights.[49]

The effectiveness and proportionality of available measures should play a role in selecting the actors best placed to tackle illegal content. Some intermediaries (eg domain name registries) may be able to take certain measures against unlawful content. Still, such measures as the taking down of domain names are both less effective and more likely to be disproportionate than those available to other actors (eg hosting providers), who are also more proximate to the content. Therefore, measures against illegal content should be targeted primarily at actors who can take proportional action. In principle, more remote intermediaries should not be targeted, or they should be targeted only as a last resort. We have previously proposed this principle in a study for the Commission. This idea was adopted in Recital 26 of the proposed DSA.[50]

3. Selected non-hosting functions in the current EU framework

3.1 Intermediary functions related to the DNS

IP addresses and domain names play crucial roles in the functioning of the internet, but the ECD's intermediary liability provisions do not explicitly cover the addressing and naming functions.[51] Technically, a domain name registration, in which the registries and registrars are involved, includes some minimal element of information storage, which could be rele-

48. *McFadden* (n 37) para 82.
49. See the judgment of the European Court of Human Rights (ECtHR) in *Vladimir Kharitonov v Russia*, no 10795/14, § 46, ECHR 2020. According to the Court, 'When exceptional circumstances justify the blocking of illegal content, a State agency making the blocking order must ensure that the measure strictly targets the illegal content and has no arbitrary or excessive effects, irrespective of the manner of its implementation'.
50. See Schwemer and others (n 47), 42-45, 60-61. In this vein, Recital 26 in the proposed DSA reads: 'Furthermore, where it is necessary to involve information society services providers, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the actor that has the technical and operational ability to act against specific items of illegal content, so as to prevent and minimise any possible negative effects for the availability and accessibility of information that is not illegal content'.
51. Domain names are only mentioned in Art 2(f) ECD in the context of defining commercial communication.

vant for Article 14 ECD. However, this storage only relates to the storage of the domain name as such and the related IP address(es), as well as registrant information in the Whois database; it does not relate to the storage of content, such as a website. A domain name may *itself* infringe particular laws (eg law on trademarks), for which there would be a safe harbour benefitting the registry or registrar.[52]

If the problem consists of illegal content accessible via a domain name, a registry or registrar arguably cannot benefit from the liability exemption in Article 14 ECD because it is not storing information.[53] The *raison d'être* of Article 12 ECD might fit best for domain name services in a teleological reading, but it was clearly not drafted with the DNS in mind.[54] The services of registries and registrars do not consist of the transmission of information in a communication network; these services only provide pointers to such content through globally unique, location-independent names.[55] Therefore, domain names are sometimes called 'signposts in cyberspace',[56] and internet standards define the DNS as a support system. It may be argued that registries or registrars are too remotely related to infringing content to risk liability for infringing content in accordance with national liability standards. Nevertheless, there exists some inconclusive lower court jurisprudence.[57]

So far, there have been no references to the CJEU regarding the DNS. In the trademark-related case of *SNB-REACT*,[58] the Court addressed another question related to the addressing function, namely service related to IP addresses. From the judgment, which was rendered without an Advocate General's (AG) opinion, it is somewhat unclear exactly what type of service is being considered.[59] The CJEU rephrased the referring court's question in paragraph 40, essentially addressing the 'provider of an IP address rental and registration service', which allowed the defendant's 'customers to use domain names and websites anonymously' (para 49).[60] The CJEU held that, in any case, such service can fall under the ECD's liability exemptions provided that the respective provision's criteria are fulfilled. In the referring case, the defendant argued that it provided access to an electronic communications network together with an information transmission service. Unfortunately, the CJEU refrained from

52. Disputes about infringing domain names are also addressed in specific procedures focussing on the registrant, eg ICANN's Uniform Dispute Resolution Policy (UDRP). It could be argued that the UDRP and similar alternative dispute resolution mechanisms might mitigate liability claims.
53. The question of liability, in contrast, depends on the national liability standard.
54. In this vein, see Sebastian F Schwemer, 'On Domain Registries and Unlawful Website Content' (2018) 26(4) *Computer Law & Security Review* 281 <https://doi.org/10.1093/ijlit/eay012>; Sebastian F Schwemer, *Report on the Workshop on the Liability of DNS Service Providers under the E-Commerce Directive* [Directorate-General for Communications Networks, Content and Technology (Unit Next-Generation Internet, E3) unpublished 2020]; Maarten Truyens and Patrick van Eecke, 'Liability of Domain Name Registries: Don't Shoot the Messenger' (2016) 32(2) *Computer Law & Security Review* 327, <https://doi.org/10.1016/j.clsr.2015.12.018>.
55. Although the notion 'communication network' is essential to the scope of Articles 12 and 13 ECD, it is not further defined in the Directive.
56. National Research Council, *Signposts in Cyberspace: The Domain Name System and Internet Navigation* (National Academies Press 2005).
57. See Schwemer (n 54).
58. *SNB-REACT* (n 40). See also Sebastian F Schwemer, 'Location, Location, Location! Copyright Content Moderation at Non-Content Layers' in Eleonora Rosati (ed), *The Routledge Handbook of EU Copyright Law* (forthcoming, Routledge 2021).
59. The plaintiff argued that the defendant had registered internet domain names that were used to sell counterfeit goods, but this was disputed. It has therefore been interpreted by some as addressing domain registrars.
60. The defendant only rented out IP addresses but not domain names, as claimed by the plaintiff (para 18). This is also confirmed by a reading of the preceding Estonian decision, which notes in para 17 that '[the] Court concluded … that the defendant was only the owner of IP addresses, not the registrar or owner of websites' (Case 2-14-6942, *SNB-REACT UA*, judgment of 26 November 2018, Tallin Circuit Court Civil Chamber; unofficial translation).

giving further guidance on whether such service would qualify under Articles 12, 13 or 14 ECD, leaving it for the referring Court to verify and assess the situation (paras 50 and 52).

Regrettably, this case does not contribute to clarifying the question of whether DNS services are exempted *de lege lata*, and even for a service consisting of the rental of IP addresses, it is likely that neither exemption's conditions would be fulfilled. *De lege ferenda*, the question remains whether there ought to be such an exemption.[61] If we consider DNS actors' proximity to content risks, we need to distinguish, *inter alia*, between business and technical proximity. Indeed, it is possible that the providers of DNS-related services are in a business relationship with the parties committing an infringement. However, the problem is that registries and registrars are technically removed from infringing content, which they neither store nor transport. As a result, they usually do not know about any illegal content, as they would need to investigate how domain names are used. Moreover, there are significant proportionality issues related to the measures DNS actors can take to manage content risks. Registries or registrars can take various domain name-related measures; however, these would often be disproportionate for two reasons. First, the precision of such measures is low because a suspension affects all content to which a domain name points (eg all of wikipedia.org), which is overly broad. Second, the suspension of the domain name only removes the 'signpost', whereas the content will typically still be available on the machine identified by the related domain names. Thus, suspension of a domain name is not a particularly effective measure for combating illegal content or information in the first place.

Historically, technical abuse,[62] such as the use of malware, has been topical in the DNS space and may be addressed voluntarily by some actors.[63] Recently, however, content-related aspects have also become more topical, as witnessed at the Internet Governance Forum 2019. When ICANN sets policies for the internet, there exists no global agreement on content, and ICANN's mission has been described as unclear but rightly hesitant in relation to content.[64]

Despite the above-mentioned conceptual distance from content, some domain registries have engaged in some form of voluntary self-regulation. There exist, for example, trusted notifier arrangements[65] both with public authorities (eg ccTLD registry Nominet with the

61. See also below in the context of the DSA.

62. On the differentiation and the notion of abuse on the DNS versus abuse of the DNS, see eg Sebastian F Schwemer, 'The Regulation of Abusive Activity and Content: A Study of Registries' Terms of Service' (2020) 9(1) *Internet Policy Review* <https://doi.org/10.14763/2020.1.1448>; and Tobias Mahler, *Generic Top-Level Domains, A Study of Transnational Private Regulation* (Edward Elgar 2019).

63. In 2020, the European Commission launched a 'Study on Domain Name System (DNS) Abuse', which is supposed to take 'a broad perspective' whereby DNS abuse can be broken down into the following categories: 'Cybersecurity threats such as Distributed Denial of Service Attacks (DDoS), Spam, Phishing, Malware, Botnets, aiming at disrupting the DNS and the internet infrastructure as well as at exploiting it to perpetrate crimes', as well as 'the distribution of illegal and harmful materials on the internet, such as child sexual abuse material, material infringing Intellectual Property Rights (IPR), sales of counterfeit drugs and other online shopping frauds' <https://ec.europa.eu/digital-single-market/en/news/study-domain-name-system-dns-abuse> accessed 9 March 2021.

64. See Mahler (n 62) ch 6. With respect to gTLDs, ICANN stands in a contractual relationship with most registries and registrars via a registrar accreditation agreement. New gTLD registry agreements contain certain obligations on registries, which stipulate, *inter alia*, that registries include a provision in registry-registrar agreements regarding prohibiting registrants 'from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name': see Mahler (n 62) ch 11.

65. See Council of European National Top-Level Domain Registries (CENTR), *Domain Name Registries and Online Content* (CENTR 2019); see also Annemarie Bridy, 'Notice and Takedown in the Domain Name System: ICANN's

Police Intellectual Property Crime Unit in the United Kingdom) and industry organisations (eg gTLD registries with the Motion Picture Association of America; gTLDs and ccTLDs in the Healthy Domain Initiative), but there is generally scarce information on their workings. Some registries also address content- or technical abuse-related aspects in their terms of service, and there exist examples of notice-and-actions arrangements.[66] The role of registration data is of special interest. Some ccTLD registries have noted a plausible correlation between domain names that are used for illegal purposes (related to content or technical abuse) and the quality of registration data. In this connection, several registries have introduced some kind of data validation process.[67] Related to registration behaviour, several DNS actors have responded to such issues as the potentially abusive registrations during the Covid-19 crisis.[68]

3.2 Wi-Fi hotspots

Today, internet cafes, hotels, public places and other establishments regularly offer Wi-Fi hotspots to their customers. Furthermore, citizens sometimes share their internet access with family members, friends or visitors. There are various business models, including the inclusion of advertisement.[69] The provision of Wi-Fi hotspots has a key function for connectivity and implies significant benefits for society, particularly as a complement to existing wireless offers (eg 4G) and future 5G networks.[70] This can be illustrated by the fact that the provision of Wi-Fi hotspots and the related intermediary liability question has also been mentioned, for example, in both the public consultation[71] and the Commission's proposal[72] which lead to Regulation (EU) 2017/1953 on the promotion of internet connectivity in local communities.

CJEU jurisprudence on Wi-Fi hotspots has its basis in German cases, so we need to present briefly the national legal context, which may differ significantly from the contexts of other Member States. In 2010, the German Federal Court of Justice (Bundesgerichtshof) held that 'a private person operating a Wi-Fi network with internet access may be regarded as an "interferer" ("Störer") where he has failed to make his network secure by means of a password and thus enabled a third party to infringe a copyright or related right'.[73]

Ambivalent Drift into Online Content Regulation' (2017) 74(3) *Washington and Lee Law Review* 1345; and Sebastian F Schwemer, 'Trusted Notifiers and the Privatization of Online Enforcement' (2019) 35(6) *Computer Law & Security Review* 105339 <https://doi.org/10.1016/j.clsr.2019.105339>.

66. In the context of ccTLDs, see Schwemer (n 62); in the context of gTLDs, see Brenden Kuerbis, Ishan Mehta and Milton Mueller, *In Search of Amoral Registrars: Content Regulation and Domain Name Policy* (Internet Governance Project, Georgia Institute of Technology 2017).
67. Schwemer (n 62).
68. See eg Sion Lloyd, 'Reporting Potential Pandemic-Related Domains' (ICANN Blog 01 May 2020) <www.icann.org/news/blog/reporting-potential-pandemic-related-domains> accessed 10 March 2021; CENTR, 'The True Effect of Corona on the DNS' (CENTR News, 14 April 2020) <https://centr.org/news/blog/the-true-effect-of-corona-on-the-dns.html> accessed 10 March 2021; Giovane C M Moura and others, 'Coronavirus and DNS: View from the .nlccTLD' (2020) *SIDN Labs Technical Report TR-2020-01*.
69. This is technically becoming more difficult because most web browsers are gradually enforcing the use of encrypted communication between user and host.
70. However, the possibility exists that they might become less relevant over time with improving 4G or 5G capabilities.
71. See Commission, 'Synopsis report on the public consultation on the evaluation and review of the regulatory framework for electronic communications' (2016) 9.
72. Commission, 'Proposal for a Regulation amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of Internet connectivity in local communities' COM/2016/0589 final.
73. Bundesgerichtshof, 12 May 2010, *Sommer unseres Lebens* (I ZR 121/08), as summarized by AG Szpunar in *McFadden* (n 38) para 17.

This secondary liability[74] applies to an actor who—without being a perpetrator or participant—contributes in any way, deliberately and adequately causally, to the violation of an 'absolute right'.[75] This implies that certain obligations are extended, to some extent, to third parties ('interferers') who have not committed the infringing act. Since the secondary liability cannot be extended excessively to third parties that have not carried out the unlawful act themselves, this liability presupposes the violation of an obligation/duty of care.[76] The extent of that obligation is determined according to what can reasonably be expected from the interferer.[77] This secondary liability was applied to owners of Wi-Fi access points. The remedy typically included monetary damages, the obligation to cease current and stop future infringements, and enforcement costs. Thus, the remedies combined damages (from which intermediaries are exempted), injunctive relief and certain costs. These costs are significant because they can also have a punitive effect, as discussed below.

According to the case law of the CJEU, it is now settled that the providers of Wi-Fi hotspots benefit from the liability exemption under Article 12 ECD.[78] However, in many cases, these 'service providers' do not offer Wi-Fi-based internet access as their main line of business; instead, they do so in their private capacity or ancillary to other businesses, which makes it challenging to achieve a fair balance of fundamental rights. As illustrated by the case law of the CJEU, problems related to the provision of Wi-Fi hotspots often occur in the context of intellectual property rights infringements committed by users of such hotspots. This includes situations in which the hotspot is unsecured, facilitating the use (and the commission of illegal acts) by potentially anonymous third parties.

What can be expected from Wi-Fi hotspot providers? In the *McFadden* case, the CJEU discussed the different types of measures that could be expected from the provider of a Wi-Fi hotspot. Monitoring all information transmitted would be contrary to Article 15(1) ECD[79] and terminating internet connection would infringe freedom to conduct business.[80] In contrast, requiring password protection strikes a balance in the view of the CJEU: it is sufficiently effective and targeted to protect against further infringements, and it does not damage the essence of the right to freedom to conduct business or freedom of information.[81] Regardless, this raises the question of whether injunctions on 'mere conduit' intermediaries should be delimited at the EU level. The objective with injunctions is to require the service provider to terminate or prevent an infringement. This is different from liability, which may serve restitutionary and punitive purposes.

---

74. Also sometimes referred to as 'indirect liability': see eg ibid para 71.
75. This means an absolute right in the sense of an exclusive right, eg copyright, based on the notion in German law. Bundesgerichtshof, 26 June 2018, *Dead Island* (I ZR 64/17) para 15. See also Spindler (n 28).
76. Bundesgerichtshof ibid.
77. ibid. Such an obligation may include the securing of a Wi-Fi access point: see Bundesgerichtshof, 12 May 2010 in *McFadden* (n 37) para 17.
78. *McFadden* (n 37).
79. ibid para 89, with further references.
80. ibid para 88.
81. ibid paras 100 and 91. The CJEU did not follow AG Szpunar in *McFadden*, who was of the 'opinion that the imposition of an obligation to make access to a Wi-Fi network secure, as a means of protecting copyright on the Internet, would not be consistent with the requirement for a fair balance to be struck between, on the one hand, the protection of the intellectual property rights enjoyed by copyright holders and, on the other, that of the freedom to conduct business enjoyed by providers of the services in question' (para 147). The AG also noted the importance of having open Wi-Fi networks, which is a significant advantage for society, outweighing the disadvantages for rights holders.

The potential of the punitive effects of injunctions has been of concern.[82] In the German cases, injunctions were procedurally based on a formal notice ('Abmahnung') issued by a lawyer, with costs to be borne by the recipient of the notice. In the leading 2010 Wi-Fi case, the claimed pre-litigation enforcement costs were more than double the claimed damages. In cases where the infringing action—for instance, copyright infringement based on peer-to-peer file sharing—was committed by a third person that could not be identified or targeted (eg a family member, visitor or business customer), the costs related to the injunction were ultimately borne by the Wi-Fi hotspot owner (the intermediary) and could have a punitive effect similar to damages for liability. As pointed out by AG Szpunar in *McFadden*, especially the punitive effect of pre-litigation costs related to injunctions may be problematic in light of the objective of the liability exemption.[83] Although the CJEU did not follow the AG's argument (to exclude pre-litigation expenses), the subsequently mentioned legislative changes in Germany, where the *McFadden* case had its origin, illustrate the significance of this point.[84]

'Mere conduit' service providers in Germany are no longer required to pay the enforcement costs related to the remedy that can be used to require the blocking of access to information. The advantage of this legislative solution is that it affords the rightsholder a mechanism to ensure the future blocking of information while avoiding the punitive effects of substantial pre-litigation costs. Particularly in the context of Wi-Fi hotspots, where service providers may also include private individuals and small businesses, this relates to the interests and fundamental rights of individuals and entities that offer such 'services' in the context of private and family life or simply as an accessory to other business activities. An exhaustive comparative analysis is outside the scope of this article, but if the punitive effects of injunctions targeting Wi-Fi owners are also a problem in other Member States, a harmonised EU approach may be advisable.

Under Article 7 of the Charter of Fundamental Rights of the European Union, persons belonging to the same family may, as such, benefit from special protection allowing them not to be compelled to comply with an obligation requiring them to incriminate one another, where one or another of them is suspected of having committed an illegal act.[85] However, EU law[86] precludes national legislation, under which 'the owner of an internet connection used for copyright infringements through file-sharing cannot be held liable to pay damages if he can name at least one family member who might have had access to that connection,

82. The Commission deemed that 'large scale use of injunctions as part of a general policy to fight against illegal content rather than being used against a specific infringement' is problematic. See 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', COM(2003) 702 final, 12.
83. AG Szpunar in *McFadden* (n 38) para 77.
84. Germany amended its transposition of the ECD in both 2016 and 2017, addressing the provision of Wi-Fi access with a view to limiting secondary liability. A detailed presentation of the status in Germany is beyond the scope of this article.
85. Case C-149/17, *Bastei Lübbe GmbH & Co KG v Michael Strotzer*, judgment of 18 October 2018 (ECLI:EU:C:2018:841) para 49.
86. Article 8(1) and (2) of Directive of the European Parliament and of the Council 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10 ('InfoSoc Directive') read in conjunction with Article 3(1) thereof, and Article 3(2) of Directive of the European Parliament and of the Council 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L 157/45 ('Enforcement Directive').

without providing further details as to when and how the internet was used by that family member'.[87]

Although this has not been highlighted in case law, it is not always clear that all providers of Wi-Fi hotspots provide an information society service (ISS). It is questionable, for example, whether private hotspots provided for family members and friends fulfil the economic requirements of ISSP or whether a Wi-Fi service is always supplied 'at a distance'. While these concepts can be (and often are) defined in a way that includes Wi-Fi hotspots, this also raises the more general question of the usefulness of the ISSP concept for the context of intermediaries (including individuals) facilitating communication in a network.

3.3 CDNs

A CDN is a geographically distributed network of both (traditional) caching and reverse proxy servers and data centres that improves the efficiency of the delivery of content to end users. Practically, CDNs solve the need to maintain a large number of specialised caching proxy servers in data centres all over the world and the need to store large media files, such as video content, on servers either in the same data centres as the caching proxy servers or in similar data centres in close physical proximity to users. The technical setup of CDNs is complex and can vary. Two functions of a CDN service provider can be distinguished for their legal assessment: first, they can provide traditional caching service to benefit IAPs based on content requests from users; second, CDN service providers can act on behalf of content owners by moving some of the reverse proxy functions from the data centre of the origin host (hosting in the sense of Article 14 ECD) to data centres at the edge of the network, where CDN equipment is located. The CDN servers become surrogate hosts and can offer both caching of unencrypted content and temporary content hosting at the edge of the network as a service to the host provider; this can also comprise content adaptation services, including encrypting the content using a digital certificate identifying the content owner.

In addition to traditional caching of potentially illegal information, such functions as surrogate hosting and content adaptation could raise some questions on the applicable conditions of the liability exemption if some part of the content in the CDN is illegal. Below, we concentrate on the CDN service on behalf of a content owner. This aspect relates to the question of how the CDN can be integrated into the communication between a content owner and end users. The use of a reverse proxy enables a CDN to distribute the requests of end users to either the cached or the original content.

In practice, CDNs use the DNS as the mechanism for this function. A simple way of handling this is for the content owner (registrant of a domain name) to use the authoritative DNS name server of the CDN provider. As a result, the reverse proxy used by a CDN is 'fronting the host' with an IP address of the CDN. This enables the CDN's DNS name server to respond with the IP address of the reverse proxy with the shortest distance to the user looking up the IP address of the domain name. One relevant technical consequence of this setup is that the IP addresses of the CDN's reverse proxy become the IP addresses of the domain name in the lookup. In other words, the IP address(es) of the host is (are) not visible to the end user. This can be compared to the 'care of' (c/o) or post office box in the analogous world of letter mail, where the sender does not know the address of the recipient, but the

87. *Bastei Lübbe* (n 85) para 55.

item is rerouted to a post office. In relation to this consequence, one prominent CDN service provider, Cloudflare, was included in the Commission's Counterfeit and Piracy watch list in 2018 because CDNs can 'provide anonymity to the operators of pirate sites' and 'hide the original IP address of the site which actually hosts the content'.[88]

CDN services are often combined with additional related services, such as DNS resolvers, cybersecurity services[89], hosting or domain registrar services. Today, the use of CDNs is widespread and relied on by a large number of lawful and unlawful services. Given the range of CDN business models consisting of a variety of complex functions, the CDN notion would not be useful as a legal concept. Instead, it is necessary to differentiate between the respective services and functions, which may fall under different liability exemption rules.

Given the increased practical importance of CDNs, it is of interest to assess their role in the intermediary liability regime of the ECD. The availability of liability exemptions has also been identified to be of major business importance to CDN service providers.[90] Generally, there exists little jurisprudence on CDNs and the related technical functions. However, in 2019 and 2020, Cloudflare was subject to several lower court proceedings in EU Member States in the context of injunctions.[91]

A CDN provider can guarantee the availability of a website, even when a customer's website is temporarily inaccessible. This relates to hosting, which is covered under Article 14 ECD and not further explored here. The traditional caching aspects of CDNs (on behalf of IAPs) qualify for the liability exemption in Article 13 ECD. Only if a CDN performs content adaptation is the availability of a liability privilege uncertain. This uncertainty emerges because of the requirement not to modify the information. Modifications to the *representation* of information will likely be unproblematic, whereas modifying the *content* may void the liability exemption.[92]

When the CDN provides a service to the content owner (ie not the IAP), it functionally becomes a 'surrogate host' and can offer both caching of unencrypted content and temporary content hosting at the edge of the network. In addition, the use of a reverse proxy enables a CDN to distribute the requests of end users to either the cached or the original content as load balancing. As a result, the reverse proxy used by a CDN is 'fronting the host' with an IP address of the CDN. This enables the CDN's DNS name server to respond with

88. European Commission, 'Counterfeit and Piracy Watch List', SWD(2018) 492 final. In the German Cloudflare case (see below), the court underlined that this business model, however, is not based on the promotion of copyright infringements.
89. Eg Distributed-Denial-of-Service (DDoS) attack protection, which is a further function of reverse proxy servers.
90. In its quarterly report to the US Securities and Exchange Commission (SEC), Cloudflare noted in relation to business risks: 'Our customers may use our platform and products in violation of applicable law or in violation of our terms of service or the customer's own policies. The existing laws relating to the liability of providers of online products and services for activities of their users are highly unsettled and in flux both within the United States and internationally'. See Cloudflare, *Quarterly Report to the United States Securities and Exchange Commission*, Form 10-Q, quarterly period ending 30 September 2019, 57.
91. *Mediaset (RTI) v Cloudflare*, order of Rome Commercial Court dated 13 March 2019, no 1932/2019 and confirmed in *Mediaset (RTI) v Cloudflare*, order of the Rome Commercial Court dated 24 June 2019, no 26942/2019; Cologne District Court, case 14 O 171/19, 30 January 2020, *Universal Music GmbH v Cloudflare*.
92. Compare Recital 43 ECD. This only exempts manipulations of a technical nature, which take place in the course of transmission, because they do not alter the integrity of the information contained in the transmission. In this context, the distinction between 'information' and 'data' prevalent in informatics may also play a role. It could be said that all content adaptation changes the communicated data (ie the signs), but not all content adaptations modify the information (the meaning of the data). See further Lee A Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight' (2015) 35(1) *Oxford Journal of Legal Studies* 91 <https://doi.org/10.1093/ojls/gqu011>.

the IP address of the reverse proxy with the shortest distance to the user looking up the IP address connected to the domain name. This use of a reverse proxy is not covered by Articles 13 or 14 ECD, as it is different from storage (although it could be combined with storage). To be exempted under Article 12, the service would have to consist of transmission in a communication network. However, the reverse proxy is arguably not engaged in the data transmission, but can instead be said to facilitate content delivery by fronting the host with the IP address of the CDN (which is connected to the domain name of the content owner). Even if one conceptualises data transmission broadly, such that it would include reverse proxies, a CDN may engage in the selection of recipients, which would void Article 12. Therefore, it could be argued that no liability exemption is available de lege lata for the reverse proxy mechanism. This could be seen as an unintended consequence, given the significant benefits offered by CDNs and their role as an intermediary between the content owner and the end user. Given that CDNs employ various mechanisms for content delivery, it is possible that the same conclusion would also apply to other technological solutions not addressed here or developed in the future.

To tackle this gap (at least for the use of reverse proxies by CDNs), the lawmaker should consider extending the existing safe harbour provisions, taking into account the degree of control CDNs have over content risks. CDNs have a high business proximity to the content owner because it is most likely a customer of the CDN. The CDN's reverse proxy function is closely related to the content owner, even when it does not store the content. By distributing user requests to various locations where the content is available, the CDN acts as a 'surrogate host'. To some extent, the situation of the CDN is similar to the hosting regulated in Article 14 ECD, except that the CDN does not (necessarily) store the data. When a CDN is employed, users viewing the web page www.example.com are sent to the CDN's IP address, via which the content is delivered or provided. CDNs often also encrypt content using a digital certificate identifying the content owner, thereby increasing the business and technical proximity. At the same time, CDNs are arguably unaware of the possible illegality of the content they distribute. If Article 14 ECD were modified to intermediary services that provide (rather than store) the information, such CDN services would arguably be covered by an amended Article 14. Similarly, Article 13 ECD could be amended to cover the 'intermediate and temporary provision of content', which might be more suitable given the temporal dimension. As a consequence, the reverse proxy used by CDNs and similar solutions would be exempted from liability subject to the conditions of either Article 13 or 14 ECD. The consequences of the respective conditions require further analysis. However, two caveats need to be mentioned with respect to this solution. First, a narrow interpretation of the active/passive criterion might inhibit the solution delineated above, so this would require further analysis. Second, the envisaged extension of Article 13 or 14 ECD would also require further scrutiny because it might have unintended side effects for other services that are not considered here.

There is generally limited information on the self-regulation of CDN providers. From anecdotal evidence, it appears that some CDN service providers may also make content- or use-related decisions based on the enforcement of the terms of service (ToS) with customers.[93] At the company level, Cloudflare has a trusted reporter programme in place in

93. In 2017, for example, Cloudflare dropped DDoS protection for the right-wing website The Daily Stormer as a customer, following the lead of other intermediaries in light of public pressure against the provision of services to the website. See 'Daily Stormer: Cloudflare Drops neo-Nazi Site' *BBC* (London, 17 August 2017) <www.bbc.com/news/technology-40960053> accessed 10 March 2021.

relation to CSAM.[94] According to the German Cloudflare case, this also exists with music rights holders.[95]

3.4 Processing in the cloud

Remote processing operations carried out in cloud computing and other contexts imply the possibility that the service provider is involved with processing illegal content.[96] Similarly, the remote processing of illegal information may also be problematic in other scenarios, such as with respect to content adaptation, for example, in a CDN context. Content adaptation can be divided into two categories that involve either modifying the representation of the content or the content proper.

'Cloud computing' is used as a label for a variety of business models that primarily offer the use of resources in data centres. A 'cloud computing service' can be defined as a 'digital service that enables access to a scalable and elastic pool of shareable computing resources'.[97] Further characteristics include self-service and metered provision, meaning one only pays for the resources one is using.

Within the liability exemptions of the ECD, it is not easy to locate all services offered in a cloud setting. Under Article 14 ECD,[98] the service provider is not liable for the information stored at the request of a recipient of the service. Storage of information is certainly relevant in cloud settings, but the stored information is often encrypted, which makes notice-and-action challenging.[99] In addition, the relatively complex cloud business models typically go far beyond the storage of information. Services involving the processing of data (thus going beyond storage) include infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Cloud-based data processing can have a variety of use cases, including the Internet of Things (IoT) and robotics.

A first question, as mentioned above, is whether cloud processing services can be seen as separate from storage, in the sense that these would be separate actions for which the service provider could be liable. There is no clarity on whether the performance of processing services could be taken as an argument for constituting liability, separate from the argument for the storage of information. It may be argued that the processing is carried out in close relation to the storage function and constitutes some form of 'enhanced hosting' with some extra services. In contrast, Article 14 does not explicitly include wording that would include other (eg processing-related) functions in the safe harbour it provides.[100] Thus, one would have to identify a separate liability exemption for such function. This second question depends on an interpretation of Articles 12 and 13 ECD.

None of the specific liability exemptions of the ECD seem directly to encompass remote processing operations. Potentially, it could be envisaged that a protection may nevertheless

94. See Doug Kramer and Justin Paine, 'Cloudflare's Response to CSAM Online' *Cloudflare* (The Cloudflare Blog, 6 December 2019) <https://blog.cloudflare.com/cloudflares-response-to-csam-online/> accessed 10 March 2021. Cloudflare is also a partner in the INHOPE Network.
95. There appears to be no public information available on this arrangement.
96. The challenges with processing in a cloud context were also highlighted in van Hoboken and others (n 42) 15.
97. Article 4(16) NIS Directive. A more precise term than 'shareable' might be 'multi-tenant'.
98. Part of the literature sees Article 14 ECD as most appropriate for cloud services: see eg Jasper P Sluijs, Pierre Larouche and Wolf Sauter, 'Cloud Computing in the EU Policy Sphere' (2012) 12(3) *JIPITEC* 12 <https://doi.org/10.2139/ssrn.1909877>.
99. See eg GSM ETNO, *Position Paper on the Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online* (July 2019).
100. Weber argues that Article 14 is based on an 'inflexible' definition. See Rolf H Weber and DN Staiger, 'Cloud Computing: A Cluster of Complex Liability Issues' (2014) 20(1) *Web JCL*.

be found by interpretation of the ECD's liability exemptions, eg based on a general analogy. Alternatively, a teleological interpretation of some of the aims of the ECD could lead to an expansive interpretation, encompassing services offered that are similar to those covered in Articles 12 to 14, or which are offered in conjunction with such services (in particular, Article 14). However, such general arguments for extending the scope of the liability exemptions, *de lege lata*, could be difficult because they are based on specific conditions that are closely related to the respective specified function. It would be unclear which conditions would apply to services not explicitly covered currently by the ECD. For example, the requirement that the information cannot be modified clearly appears to be of limited utility in the context of remote processing (including adaptation of the content). Furthermore, such processing is usually not visible to the service provider, particularly if encryption is used and when there are several layers of cloud computing. Concomitantly, we recommend that the European lawmaker address the exemption gap for remote processing operations, as well as the possibility that new business models offer functions that do not fit into the existing limitations.

3.5 Live-streaming

Live-streaming has recently become more topical than it was before, both in a commercial context and in the context of illegal or harmful content. The internet supports multicasting, that is, one-to-many communication by streaming content to a group of receivers in a single transmission. In principle, live-streaming without intermediaries storing the content is technically possible. However, in practice, live-streaming is a service that usually provides simultaneous storing and real-time streaming of an event, and live-streaming will use the same CDNs that are used for streaming stored content. There are many service providers offering a technical platform and hosting service for live-streaming.

Because live-streaming involves an event that is transmitted in real time, the party initiating the streaming will start transmitting when the event starts. This party may decide to publish the recorded event as an ordinary streamed video as soon as the real-time event terminates. Users obtain access to the live stream by requesting to receive the transmission. Live-streaming is also part of the content offered by social media services like Facebook and Twitter, and live-streaming content may be suggested to anyone using these services. Many-to-many live-streaming is also supported by many service providers, and this service is usually called video conferencing.

Live-streaming can be a type of linear audio-visual media service that is regulated in the revised AVMSD. This Directive addresses video-sharing platform services, including both non-linear (on demand) and linear services, which arguably include live-streaming.[101] The revised AVMSD (Article 28b) requires providers of video-sharing platforms to take appro-

101. On such a service, videos are shared and the organisation of the sharing is determined by the provider. The wording speaks of a service that is devoted to 'providing' programmes, user-generated videos or both to the public. In the drafting history of the revised AVMSD, the word 'providing' replaced an earlier proposal focussing on 'storage or live streaming'. While the 2010 AVMSD classified live-streaming as television (Recital 27), the 2018 AVMSD, emphasises in Recital 9 that 'the procedures and conditions for restricting freedom to provide and receive audiovisual media services should be the same for both linear and non-linear services'. See references in Nadia Feci, 'Gamers Watching Gamers: The AVMSD Soon the One Calling the Shots?' (*KU Leuven CiTiP*, 18 December 2018) <www.law.kuleuven.be/citip/blog/gamers-watching-gamers-the-avmsd-soon-the-one-calling-the-shots/> accessed 11 March 2021. See also Commission, 'Communication from the Commission: Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive 2020/C 223/02 [2020] OJ C 223/3.

priate measures to address incitement to violence and some forms of hatred against individuals or groups. In addition, the providers need to protect the public from content that is illegal under Union law (related to terrorism, child abuse images, racism and xenophobia). The AVMSD explicitly states in Article 28a(5) that Articles 12 to 15 ECD apply to video-sharing platform providers.[102]

In the context of the ECD, live-streaming is difficult to locate, and relevant case law is scarce. Functionally, live-streaming is similar to hosting, but it likely does not qualify as such under Article 14 because the streamed content is not stored before the communication but streamed in a linear manner. Technically, live-streaming involves some element of transmission in a communications network ('mere conduit'),[103] but the nature of the service may be different from the one envisaged by Article 12 because of temporal and functional characteristics.[104] The default situation for mere conduit is the instantaneous communication of data in a network, which is over when the data are communicated. Thus, by the time a notice is issued, the communication is already over. In the case of live-streaming, content is continuously streamed for a limited time. This is somewhat comparable to hosting because the live-streaming service 'hosts' the live-stream. However, this is not necessarily using a stored file (like in hosting), but a continuous content stream. Thus, notice-and-action may be possible, and certain measures are obligatory under the AVMSD. Live-streaming may also involve a temporary storage of content (Article 13 ECD), but it is uncertain whether the provider does so 'for the *sole* purpose of making more efficient the information's *onward* transition'.[105] Moreover, an eventual liability might be based not (only) on the temporary storage but on the streaming (the provision of access to the streamed content), for which no dedicated exemption exists.

Underlying this is also the question whether live-streaming falls under the ECD regime in the first place. The ISS definition requires that such a service is 'at the *individual request* of a recipient of services'.[106] It could be argued that this criterion is not fulfilled in the case of live-streaming, which resembles broadcasting.[107] At the same time, the criterion could be fulfilled if the streamer (the person initiating the streaming) were seen as the recipient of the service, but this makes it difficult to distinguish between streaming and broadcasting. Moreover, the live-streaming provider can select the viewer of the live stream—that is, the receiver of the communications—for example, based on algorithms that evaluate the users' interests. This can be the case with respect to existing live-streaming services, such as Facebook and YouTube, but it would arguably void the protection afforded by Article 12(1)(b) ECD. Therefore, under a narrow reading of the ECD, at least some instances of live-streaming may be protected neither under Article 12 or Article 14 ECD.

A future regulation could address the gap, taking into account the control the service provider reasonably has over the content-related risks. A live-streaming services provider has

102. Moreover, according to Article 28b(3), second subparagraph, such measures shall not lead to any *ex ante* control measures or upload-filtering of content, which do not comply with Article 15 ECD.
103. See also Jan Bernd Nordemann, *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?* Study prepared for the European Parliament (IP/A/IMCO/2017-08, 2018) 13.
104. On the temporal aspect, see *McFadden* (n 37) para 62.
105. Article 13(1) ECD, emphasis added.
106. Emphasis added.
107. Broadcasting under the AVMSD may be subject to further requirements, such as license to operate. The Technical Standards Directive indicates this in Annex I services, which are not considered to be supplied 'at the individual request of a recipient of services', namely '[s]ervices provided by transmitting data without individual demand for simultaneous reception by an unlimited number of individual receivers (point to multipoint transmission)', including 'television broadcasting services (including near-video on-demand services)', 'radio broadcasting services' and '(televised) teletext'.

a relatively close proximity to the content compared with typical mere conduit providers. Technically, the live-streaming provider is directly or indirectly connected to the live stream because the streamer is most likely its customer. Moreover, as foreseen in the AVMSD, these providers of video services are in a position to manage some aspects of the live-streaming they organise. At the same time, a service provider cannot be expected to have knowledge of everything happening on its service in real time.

Live-streaming providers might be able to take certain measures. Providers can be notified of an infringing live stream and react to such a live stream (eg take it down), at least while it is still continuing. Providers' failures to react to notices were among the criticisms voiced after the terrorist attack in Christchurch, New Zealand, in 2019. There is limited systematic information on the self-regulation of live-streaming, although this has substantially increased in importance following the Christchurch attack.[108]

It is unclear whether providers might technically be able to engage in *ex ante* monitoring, which would be problematic from a fundamental rights perspective. If mandated, it would have to comply with the prohibition of 'general' monitoring obligations in Article 15 ECD. This temporal aspect is challenging from a regulatory perspective because the service provider needs to act in a timely fashion, and it may be difficult to ascertain whether a certain live-stream contains illegal material. Therefore, a regulation would need to provide possibilities for the service provider to act expeditiously, while at the same time, respecting fundamental rights. It is not clear how this challenge can be resolved going forward.

3.6 Search engines

Search engines,[109] or information location tool services, and hyperlinks[110] are other areas of interest related to the delimitation between Articles 12, 13 and 14 ECD. They are also explicitly mentioned in Article 21(2) ECD, a provision in relation to which the Commission was called upon to examine the 'need for proposals concerning the liability of providers of hyperlinks and location tool services'. A closer examination of this is outside the scope of this article, but it should be noted that several Member States have included specific liability exemptions for these services in their national legislation.[111] In Austria and Liechtenstein, for example, the liability exemption for search engine services and hyperlinks follows Article 12 ECD. Spain, Portugal and Romania have enacted such liability exemption for search engines and hyperlinks modelled after Article 14 ECD.[112] In *Google France*, the CJEU applied Article 14 ECD in the advertising context of search engines, Adwords.[113] In relation

108. See also Tech against Terrorism, *Analysis: New Zealand Attack and the Terrorist Use of the Internet* <www.techagainstterrorism.org/2019/03/26/analysis-new-zealand-attack-and-the-terrorist-use-of-the-internet/>accessed 11 March 2021.
109. An 'online search engine' is defined, for example, both in Article 4(18) NIS Directive and Article 2(5) Regulation (EU) of the European Parliament and of the Council 2019/1150 on promoting fairness and transparency for business users of online intermediation services [2019] OL L 186/57.
110. In the context of copyright, the CJEU has interpreted hyperlinking in Case C-466/12, *Nils Svensson and Others v Retriever Sverige AB*, judgment of 13 February 2014 (ECLI:EU:C:2014:76); Case C-348/13, *BestWater International GmbH v Michael Mebes and Stefan Potsch*, order of 21 October 2014 (ECLI:EU:C:2014:2315); and Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others*, judgment of 8 September 2016 (ECLI:EU:C:2016:644).
111. In addition, the copyright-specific US-American counterpart to the ECD's liability exemptions in DMCA § 512 contains a specific exemption for 'Information Location Tools'.
112. Commission, First Report (n 82) 13.
113. *Google and Google France* (n 40) paras 114ff. On the question of search engines and Article 14 ECD outside the advertising context, see Hoboken and others (n 42) 34; Nordemann (n 103) 15-16.

to data protection, the CJEU interpreted Data Protection Directive 95/46/EC to contain a ground for removal—that is, de-indexing—of search results in *Google Spain*,[114] now codified in Article 17 GDPR; however, it did not take a stance on search engines' position with respect to the ECD. A comprehensive overview of national case law on the matter is outside the scope of this article. Despite stark differences in consequences under Article 12- *vis-à-vis* Article 14-akin national regimes, the Commission did not see a risk for fragmentation in the internal market in 2003.[115] Still, this grey area might be of interest when reviewing the ECD.[116]

4. Filling in the missing parts of the liability exemption regime going forward

The ECD was adopted more than twenty years ago. The non-hosting examples analysed in this article have so far generally—but to varying degrees—given little rise to case law before the CJEU. At the same time, the landscape of non-hosting intermediaries has developed significantly since the adoption of the ECD, for example, with regard to the development from caching to CDNs and content adaptation, as well as developments related to cloud computing. We conclude that, despite rapid technological developments, the focus of and the rationale for the intermediary liability exemption regime in relation to non-hosting intermediaries have aged well. However, the above analysis of certain selected non-hosting functions related, for example, to the DNS, CDNs, processing in the cloud and live-streaming, has revealed that clarifications and upgrades are advisable or necessary to a varying extent. Certain non-hosting functions appear to fall through the cracks, for example, because they do not fit properly in the current regime. Notably, this relates both to *relatively new* intermediary functions and *old* established intermediary functions (eg related to the DNS), which may be uncertain under the current liability exemption regime.

The importance of the liability exemption framework is underlined by the fact that intermediaries' response to illegal content or information on the internet is influenced by, *inter alia*, the respective liability conditions, which vary greatly between 'mere conduit' and hosting. As shown, some non-hosting actors rely on notice-and-action mechanisms, which we know from the hosting/platform discussion. However, voluntary measures should also be subject to transparency obligations and procedural safeguards, and effective remedies should be available for users to safeguard fundamental rights.[117]

The current European framework and its proposed upgrade in the form of the DSA are characterised by several properties that contribute to legal certainty, such as their horizontal nature and focus on illegal content rather than unclear notions, such as harmful or abusive

114. Case C-131/12, *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* judgment of 13 May 2014 (Grand Chamber) (ECLI:EU:C:2014:317). In his Opinion in the case, AG Jääskinen explicitly referred to the liability exemption regime of ECD and commented on the analogous application of the ECD's liability exemptions on internet search engine providers: Opinion of AG Jääskinen (n 38) paras 37-38. However, this was not taken up by the CJEU in its decision.
115. Commission, First Report (n 82) 14.
116. Search engines were mentioned, for instance, in the online platform definition in the Commission's Public Consultation on 'Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy', 24 September 2015.
117. Consider the framework for actions in relation to transparency and procedure in Commission Recommendation 2018/334 (n 6) and its applicability to voluntary arrangements; see also the Santa Clara Principles <https://santaclaraprinciples.org> accessed 10 March 2021.

content. It is also important to underline that the European framework is directed at certain specific intermediary functions, not actors. Notably, the existing liability exemptions are proposed to remain largely unchanged, which would further cement this classification.[118] From a legal certainty perspective, this is preferable to, for example, a 'sliding scale' without clear conditions.

Intermediaries fulfil important societal functions that structurally limit their ability to take proportionate and effective measures to control all risks related to illegal content, without negative effects on an open and free internet. In this respect, Article 15 ECD is a cornerstone of ensuring a fair balance of interests and rights, including fundamental rights. Yet, today, the ECD lacks a foundation for intermediary liability exemptions that would open for a teleological interpretation, for example, based on a proportionality principle, meaning that more remote intermediaries should not be targeted or only be targeted as a last resort.[119]

An upgraded liability exemption regime should be future proof and become even more technology neutral, thereby increasing its shelf life. A level playing field and uniform interpretation may be ensured by a Regulation (as opposed to a Directive) as proposed. Appropriate liability exemptions should be based on clear criteria. Addressed intermediary functions should be kept technology neutral and flexible while ensuring legal certainty. If possible, the focus ought to be on abstract criteria—that is, on 'what is done' rather than 'how it is done'. Furthermore, conditions of liability exemptions should be differentiated from obligations on service providers, as foreseen in the proposal for the DSA.

The current ECD liability exemption regime, as well as the proposed update in the form of the DSA, focus on transmission in, or access to, a communication network and storage. Significant grey areas arise in two dimensions. First, 'auxiliary network intermediary' functions do not transmit data in a communications network or provide access to these.[120] Thus, these functions do not easily fit into 'mere conduit' ('direct network intermediary' functions) or other categories. Second, the 'temporary provision and processing of information' is different from storage, so it may not qualify as hosting.

On the first point, the liability exemption regime for these more remote—that is, auxiliary—network intermediaries (eg related to provision of domain names and domain name-related services, IP addresses, client software, etc)[121] is currently unclear. This could be resolved either by introducing a general liability exemption principle (for all network intermediaries outside existing categories), introducing a specific exemption for 'auxiliary network intermediaries',[122] or adopting a hybrid approach representing a combination of both.

Criteria for assigning conditions and obligations could be based on the degree of control. Relevant parameters include the service provider's proximity to the content risk and the

118. Compare Articles 3–5 DSA proposal.
119. See, however, Recital 26 DSA proposal, as discussed above.
120. As we suggested to the Commission, a definition of auxiliary network intermediary functions could be 'a service that does not fall into any of the remaining categories of intermediary functions. Such service supports the functions of other intermediaries, for example, by facilitating an underlying logical architecture and addressing system of networks, or offering software or services that enable or improve the functions of other intermediaries.' See Schwemer and others (n 47), along with considerations for drafting available at SSRN <http://ssrn.com/abstract=3810963>. Recital 27 DSA proposal partly relies on this wording without introducing a designated liability exemption.
121. Search raises specific issues and should not be included here.
122. Such an exemption could be based on Article 12 ECD and take into account the low degree of control of these functions.

availability of proportional mechanisms for managing risk (see above). Actors with limited or no control over content risk should be exempted with few/no conditions. Actors with more control over content risk should be exempted only based on more extensive conditions, subject to specific obligations.[123] Furthermore, non-exhaustive lists of examples in clarifying recitals for each category may contribute to technological neutrality while maintaining legal certainty.[124] In the recent DSA proposal, the European lawmaker indeed appears to attempt this by acknowledging in Recital 27 that 'new technologies have emerged that improve the availability, efficiency, speed, reliability, capacity and security of systems for the transmission and storage of data online, leading to an increasingly complex online ecosystem'. The recital goes on to recall that 'providers of services establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions, can also benefit from the exemptions from liability set out in this Regulation, to the extent that their services qualify as "mere conduits", "caching" or hosting services'. In this context, Recital 27 provides a non-exhaustive list of examples, including services related to Wi-Fi, the DNS, top-level domain name registries, certificate authorities, CDNs, Voice over IP, messaging and web-based e-mail. However, given that the existing liability exemptions for 'mere conduit', 'caching' and hosting remain largely unchanged, the recital seems to add little legal certainty against the background of the challenges identified in this article.

On the second point, remote (cloud) processing does not currently appear to be covered by existing exemptions in the ECD. This also applies to 'content adaptation', where the content *as such* is modified. Modifying the representation of content in the context of caching *might* be covered by Article 13 ECD. These services are desirable in the digital society and enable new innovations and business opportunities, including those with a focus on IoT. Furthermore, the liability exemption for the 'provision' of information (other than storage, ie hosting) is unclear. As a possible result, as argued above, certain CDN and live-streaming services appear to fall outside the scope of current and proposed liability exemptions, *inter alia*, because they might not store the information. If there are good reasons for exempting these non-hosting functions, these issues could be remedied by introducing a liability exemption for the 'temporary provision' and 'processing' of information.[125]

In addition to the liability exemptions framework, the DSA proposal also introduces certain novel due diligence obligations, which are to be seen as separate from but related to the liability exemptions. These obligations increase gradually from 'intermediary services' via 'hosting services' and 'online platforms' to 'very large online platforms'. At first glance, it seems that services related to non-hosting could indeed fall under the broad notion of 'intermediary service'. However, a closer look at the proposed definition reveals that the definition of 'intermediary service' relies on the notions of 'mere conduit', 'caching' and hosting.[126] Given our analysis of potential difficulties in fitting some non-hosting functions in these 'boxes', it may well be that providers of certain non-hosting services would not

123. This could also be part of a recital that helps solve future unclear cases. See too Recital 26 DSA proposal.
124. For example, Wi-Fi hotspots, IAPs, IXPs, etc in the context of direct network intermediaries.
125. This needs further scrutiny and could, for example, be done in two alternative ways. First, it could involve introducing a new liability exemption with appropriate conditions depending on the degree of control, for example, inspired by the *current* Article 14 ECD. This could be used for remote cloud processing and content adaptation in the form of modification of content as such, as well as the 'provision of information', irrespective of whether that content is stored or provided in a linear fashion or otherwise. Second, inspired by Article 13 ECD, it could be expanded to 'temporary storage or processing' and the 'intermediate and temporary provision of content'.
126. See Article 2(f) DSA proposal.

be covered by the due diligence obligations. The relevant obligations for 'intermediary services' include important duties regarding points of contact (Article 10), legal representatives (Article 11), and important transparency mechanisms regarding terms of services (Article 12) and content moderation activities (Article 13). However, in light of the goals of the proposed Regulation, it would be unsatisfactory and inconsequential if certain 'intermediary' service providers were not covered by the obligations for 'intermediary services'. Furthermore, the proposed DSA mandates trusted flagger/notifier arrangements for online *platforms* in Article 19, but in this context it also introduces important safeguards to tackle the misuse of notice-and-action arrangements (see also Article 20). Yet, in the current draft, voluntary arrangements involving non-hosting intermediaries would not be subject to the very same safeguards. As discussed, these arrangements already exist today in the non-hosting landscape. Therefore, to provide a level playing field and avoid 'a race to the most remote intermediary', it would be advisable for these safeguards and principles to apply to voluntary arrangements of any intermediary service as well.

The analysed non-hosting intermediaries—with the notable exception of internet access service providers—play a minor role in the intermediary liability landscape. Yet, they must not be overlooked. In the ongoing legislative process, the European Parliament and the Council still have the opportunity to improve carefully the current DSA proposal to create a truly future-proof regulation regarding non-hosting services.

This article is based on the authors' study undertaken for the Commission in preparation of the Digital Services Act, see Sebastian F Schwemer, Tobias Mahler, Håkon Styri, Legal Analysis of the Intermediary Service Providers of Non-Hosting Nature, Final report prepared for European Commission (2020). Considerations for drafting are available at SSRN <http://ssrn.com/abstract=3810963>. An earlier draft of this research was presented at the Global Internet Governance Academic Network (GigaNet) Annual Symposium in 2020 and the authors are thankful for the valuable discussions. The authors would like to thank the anonymous peer reviewer for the very constructive comments and Carlos J. Calleja for excellent assistance with the finalization of the paper. This research was also partly financed by the project 'Security in Internet Governance and Networks: Analysing the Law' (SIGNAL, grant number 247947), supported by the Research Council of Norway.