6

Liability Exemptions: General Requirements

6.1 Introduction

In October 1996, the European Commission published its Communication to the Council and European Parliament under the title 'Illegal and Harmful Content on the Internet'.[1] This laid the basic principles for the E-Commerce Directive (ECD) proposal unveiled in 1998. The communication stated that:

> Internet access providers and host service providers play a key role in giving users access to Internet content. It should not however be forgotten that the prime responsibility for content lies with authors and content providers. It is therefore essential to identify accurately the chain of responsibilities in order to place the liability for illegal content on those who create it … The law may need to be changed or clarified to assist access providers and host service providers, whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability.[2]

The ECD was adopted in June 2000.[3] The main purpose of its liability exemptions is to *structure* the regulation of digital services in the world's largest single market. By clarifying legal expectations, the exemptions incentivise investment in novel services. Businesses in the Member States suddenly did not have to worry about how various national laws would regulate their businesses. By aligning expectations, the ECD created

[1] Commission, 'Illegal and Harmful Content on the Internet' (Communication) COM (96) 487 final.
[2] ibid 12–13.
[3] University of Cambridge maintains a fantastic resource concerning the legislative history of the e-Commerce Directive, see Centre for Intellectual Property and Information Law, 'E-Commerce Directive' (*University of Cambridge*) <https://www.cipil.law.cam.ac.uk/resourceseuropean-travaux/e-commerce-directive> accessed 1 August 2023.

a baseline that allowed companies to expand and scale across the European Union (EU) borders.

Two decades later, the Commission concluded in its impact assessment for the Digital Services Act (DSA) that the ECD largely succeeded in achieving this goal.[4] Similarly, the 2020 evaluation report prepared for the European Parliament's Committee on Internal Market and Consumer Protection (IMCO), which I had co-authored, concluded that:

> The common liability exemption rules allow the firms to more easily scale up on the digital single market. Although far from constituting uniform rules, they give companies basic reassurances concerning the operation of their business in dealing with third-party content, and to stakeholders in enforcement of their rights. They also provide a common vocabulary for European judicial discourse. The benefits in terms of approximating the liability framework can be best seen when compared with largely the non-harmonised preventive measures.[5]

The original objective continues to remain valid today. This is now emphasised by Recital 16 of the DSA.[6] Through the DSA, the liability exemptions received a 'renewed democratic mandate'[7] from the legislatures in the EU. In 2010–20, the liability exemptions were often subject to criticism from some stakeholders that the rules were no longer 'up-to-date' or 'fit for purpose'. The oft-used argument was that most of our current digital services did not exist in 2000. While the argument was factually wrong because virtually most digital services predate the liability exemptions, it expressed a sentiment that 'many things have changed' since 2000. And obviously, many are different.

In two decades, the internet grew from a toy for experts to an essential tool used by everyone on a daily basis. Facebook (2003), YouTube (2005), and Twitter (2006) did not exist in 2000. Nor did Google's advertising system AdWords launched in the same year. With the arrival of mobile phones and IoT, digital services became much more embedded in people's lives. Thus, it is true what we understand as 'the Internet' started substantially changing *after* the ECD was enacted.

The fact that 22 years later, the co-legislators decided to only *build upon* the liability exemptions of the ECD is the greatest testimony to how future-proof the framework is. The framework arguably owes part of its success to its focus on omnipresent technical

[4] Commission, '"Impact Assessment" (Commission Staff Working Document) Accompanying the Document "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (DSA) and Amending Directive 2000/31/EC"' SWD(2020) 348 final, para 32.

[5] Alexandre de Streel and Martin Husovec, 'The E-Commerce Directive as the Cornerstone of the Internal Market – Assessment and Options for Reform' (Study Requested by the IMCO committee, PE 648.797, EU Parliament 2020) 35 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU(2020)648797_EN.pdf> accessed 1 August 2023.

[6] DSA, Rec 16: 'The legal certainty provided by the horizontal framework of conditional exemptions from liability for providers of intermediary services … has allowed many novel services to emerge and scale up across the internal market. That framework should therefore be preserved.'

[7] Interview with Irene Roche Laguna, Deputy Head of Unit for Coordination And Regulatory Compliance, European Commission (2021–23).

activities, such as storage or access, instead of chasing ever-evolving types of products and business models. However, given the ECD's early adoption, the law could say little about the regulation of various problems that might arise within digital services. The DSA tries to fill this regulatory gap.

Despite the topic's political sensitivity, the co-legislators—the European Parliament and the Council—changed the Commission's proposal only to a limited extent, having largely confirmed and even expanded it. The DSA repeals Articles 12–15 ECD and incorporates them as Articles 4–8 into the DSA. Articles 4–6 DSA—introducing liability exemptions—have largely been untouched. However, there are some minor wording changes in the context of all three exemptions. They usually extend their applicability to novel types of services.

Legally speaking, the result of Articles 4–6 DSA is that no national law can modify rules concerning hosting, caching, and mere conduit *activities*. Being a Directive, the ECD gave rise to many different transpositions and interpretations at the national level. Incorporating such rules in a directly applicable regulation is hoped to provide greater uniformity and certainty for cross-border services. The liability exemptions depict a measure of full harmonisation from which the Member States cannot deviate. Any conflicting national provisions modifying their content, even if indirectly, are automatically pre-empted by the DSA and must be set aside by a national court.[8] The pre-emptive effect of the liability exemptions is much broader (Chapter 17).

6.2 General Requirements

In this subchapter, I explore various general conditions that apply to liability exemptions. Over the years of the existence of the ECD, these conditions have been subject to growing case law and numerous controversies. The DSA has made some changes to the pre-existing case law; however, the role of the Court of Justice of the European Union (CJEU) remains key.

The EU legislature intervenes to regulate various digital services to establish and advance the Digital Single Market (DSM). The internal market rationale is not just the legal basis of the law in this area[9] but also its primary objective. The prominence of the internal market rationale is evident in the initial recitals of the instrument as well. Article 1 DSA demonstrates that the law pursues not only the goal of completing the DSM but also other goals, such as protecting the fundamental rights of victims, content creators, and other users. Because the Union legislation is based on the internal market clause, it can only regulate activities that are inherently economic.

[8] Regulation is directly applicable and takes precedence; see Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal SpA* ECLI:EU:C:1978:49. For other types of technical activities which fall outside the ambit of liability exemptions (or of the DSA), the Member States can continue to maintain or introduce their national rules, including national liability exemptions.

[9] European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1 (ECD), Rec 1; DSA, Recs 2 and 4. They share the same legal basis, art 114 TFEU (previously art 95 TEC).

6.2.1 Relevant technical activities

Liability exemptions apply to services based on the *technical activities* they perform. The qualification criteria do not consider business models or types of final products that incorporate them; they only consider the underlying technical functioning. Rules only look at whether the description of technical activities performed matches that of liability exemptions (see Figure 6.1).

This remains counter-intuitive for many. Often, it is believed that liability exemptions were designed for some types of services or even companies. This is not the case. Unlike due diligence obligations, liability exemptions are generally blind to business dimensions. Storage of third-party information can be embedded in infrastructure services (eg cloud computing) or application-layer services (eg video-sharing apps). Such services can be deployed by providers of mostly user-generated content (eg social media) or editorial content (eg newspapers, regarding readers' comments). It can be provided for a fee, free of charge, or for a different consideration (eg for a subscription or tokens). Most of the questions about how and by whom are irrelevant for the purposes of delineating the scope of technical activities.

Hosting concerns every activity that can be described as 'storage'; mere conduit any activity that can be defined as 'transmission in a communication network' or 'provision of access' to it; caching any activity described as 'transmission in a communication network' performed for the sole purpose of making its onward transmission more efficient or secure. All technical activities outside the three are outside the scope of the liability exemptions, and because of the definitional set-up of the regulation, they are also not within the ambit of the DSA (Chapter 9).

The DSA stresses that all possible future digital services should be considered under the regulatory umbrella. Recital 29 attempts to stretch the imagination of those

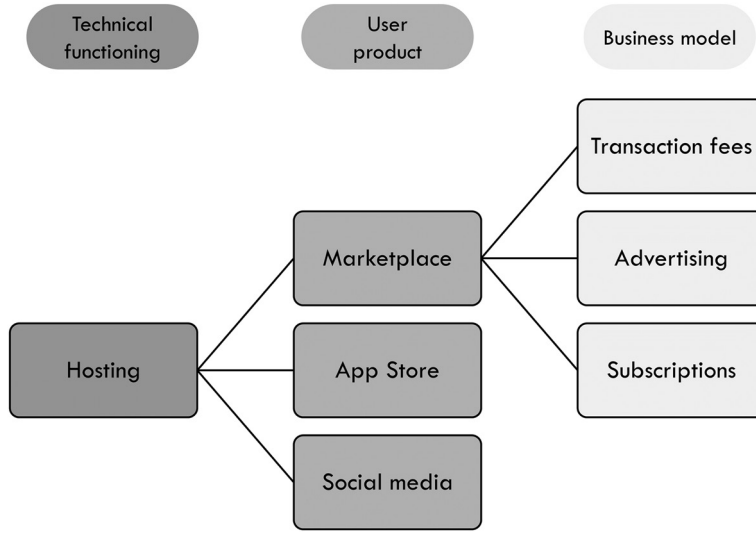

Figure 6.1 Functionality and its primacy

interpreting the law because digital services 'develop continually' and the law's reading should keep in touch with times. Therefore, Recital 29 emphasises that:

> Intermediary services may be provided in isolation, as a part of another type of intermediary service, or simultaneously with other intermediary services. Whether a specific service constitutes a 'mere conduit', 'caching' or 'hosting' service depends solely on its technical functionalities, which *might evolve in time, and should be assessed on a case-by-case basis*.[10]

Thus, although the DSA maintains the triad of existing regulated technical activities, it attempts to broaden some of them. Each regulated technical activity covers a wide range of digital services processing user-generated content that is subject to a plethora of business models. For instance, hosting, defined as the storage of third-party information, can form the core of discussion fora, video-sharing platforms, social networks, app stores, webhosting, and cloud computing services. The technical activity embedded in such services does not have to be the only activity of the service. For instance, providing access to a communication network under the mere conduit exemption can be part of hospitality services provided by hotels or be offered as a standalone service provided by telecommunication firms. In the case of composite services (Chapter 9.2), several entities might be able to invoke the liability exemption for the activity they perform together. For instance, owners of social media pages and companies might both qualify as hosting providers vis-à-vis third-party comments posted on such pages.[11]

As long as exempted technical activities can be said to constitute 'an information society service'—ie they are provided 'at a distance, by electronic means and at the individual request of a recipient of services'—in the context of what can be regarded as an economic activity, they are covered by the DSA (section 6.2.6).[12] However, the *manner* in which the technical activities are embedded in the service can influence the interpretation of conditions under which liability exemptions continue to apply. For instance, when a provider tries to present someone else's content as its own, it might disqualify itself from otherwise available liability exemptions (section 6.2.4).

6.2.2 Information 'provided by recipients'

All relevant technical activities must process 'information provided by a recipient of the service'. Thus, storage of the *provider's* information, such as when newspapers upload their own articles onto their own website, is by definition *not* covered.[13] But comments

[10] DSA, Rec 29 (emphasis mine).

[11] The Austrian Supreme Court held in 2016 that an owner of a page can qualify as a hosting provider (Case No 6Ob244/16z).

[12] See Rec 5 relying on the definition from a recast European Parliament and Council Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1.

[13] Case C-291/13 *Sotiris Papasavvas v O Fileleftheros Dimosia Etaireia Ltd and others* EU:C:2014:2209.

that their users upload in response to their articles are covered. The legal framework is meant to cover responsibility for content generated by users.
But which information exactly is said to be users' and which is said to be providers'?

Our current interpretation emphasises user-generated content services that rely on the user's *push*—an act of uploading or accessing. When users push their information onto digital services, we consider it user-generated, even if such a push requires little effort from the user's side. In contrast, when providers *pull* information from the outside world to re-organise it, we consider such services to fall outside the remit of the liability exemptions. Search engines, for instance, struggle with the current framework because they process information that presumes the website owners' consent in the absence of opt-outs. Thus, unless they have a more curated relationship with website owners, they pull user-generated content (Chapter 8).

But even among 'pushed content', it is not easy to draw the line. Most lawyers would say that Spotify is streaming its own editorial collection of music, and YouTube is providing music uploaded by its users. However, this distinction seems to rest on very small differences. Streaming services usually make available music provided by distributors—musicians' agents—who upload music.[14] The service's checks of uploaded music are not extensive. This type of content quality control is not too dissimilar from the practices of an app store which is considered a user-generated content service. Both services distribute other people's content— music or apps—for remuneration. If the streaming services cut out the distributors and allow music to be uploaded directly by authors, the difference will vanish entirely. The key to analysing these types of scenarios, therefore, seems rather how providers satisfy the condition of being provided with information discussed below .[15]

More frequently, the only kind of selection being carried out takes the form of automated sorting of information, which involves no choice. For instance, streaming services also carry podcasts. They have a much looser relationship with content creators of podcasts than those of music. As a result, for podcasts, streaming services might be regarded as hosting services of non-editorial 'provided' content while they remain distributors with regard to music. However, neutrality can be lost if the streaming service concludes an exclusive deal with one of the podcasters and their content becomes featured by the service.

As technology develops over time, it is inevitable that the struggle to define when information is still 'provided by' the recipient of the service not only remains but, in fact, gets worse. Going forward, the notion of pull and push might blur further. Which opt-outs from industry practices are a sign of push, and which are pull? Moreover, digital services will invent new ways of sorting through the available information.

[14] For more about the streaming ecosystem, Competition and Markets Authority, 'Music and Streaming Final Report' (2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120610/Music_and_streaming_final_report.pdf> accessed 1 August 2023.

[15] As explained below, this has important consequences for whether such services can become VLOPs. In my view, even non-neutral services can become VLOPs.

The emergence of generative chatbots on social media shows that automated 'user-generated' content services can entirely obscure users' genuine contributions. When users are nowhere to be seen, is the content still user-generated? In my view, the DSA has the tools to resolve these challenges. However, they need to be applied carefully. This debate is inextricably linked with the legal concept used by the CJEU to limit the applicability of liability exemptions—that of the *neutrality of a provider*. I discuss this in a separate section on the neutrality of providers below (see section 6.2.4).

Generally, any liability exemption only limits 'liability for information'. Furthermore, it limits only liability for information 'provided by the recipient of the service'. Although the DSA relies on the broad meaning of 'recipient of the service', in the liability exemptions context, the 'recipients of the service' still mostly refers to content creators who use the service to store or send information. This is logical since readers are rarely held liable for information they decide to access.[16]

Under the ECD, the recipient was usually interpreted to mean only an individual *requesting* the service, eg the end-user uploading the information or accessing a website. However, under the DSA, it is clear that anyone who '*uses* the service' can fall under the term's scope.[17] This means that both those who impart information online and those who consult the information are considered recipients. Some liability exemptions, such as those applicable to mere conduit services, can thus gain broader scope because relevant recipients now do not have to send any information. It is enough that they receive it through the service. This opens the applicability of liability exemptions to situations when users of digital services consume third-party information rather than produce it.

6.2.3 Scope of exempted 'liability'

The scope of exempted 'liability' is as broad as it gets. The broad scope is the design choice of the drafters of the ECD who wished to coordinate all possible forms of liability that could hinder the internal market. The notion thus covers all forms of criminal, administrative, and civil liability, regardless of whether imposed on providers as accessories or directly liable actors.[18] The wide scope of the term is also needed due to the horizontal nature of the liability exemptions. The intention to preserve this approach is confirmed by the DSA's broad definition of illegal content, which indicates that the liability exemptions must be 'prepared' for all kinds of illegality scenarios,

[16] One example is laws banning the possession and reading of child abuse material. See, for instance, possession of images criminalised by s 1(1)(c) of the UK Protection of Children Act 1978.

[17] Art 3(b) DSA defines 'recipient of the service' as 'any natural or legal person who uses an intermediary service, in particular, to seek information or make it accessible'.

[18] Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2020:586, Opinion of *AG Øe*, para 226. The same in the US context, see s 512(c) DMCA that 'limits the liability of qualifying service providers for claims of direct, vicarious and contributory infringement for storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider', cited from 'HR Rep No 105-551 Part 2 (1998)' at 53 (Committee on Commerce Report) <https://www.congress.gov/congressional-report/105th-congress/house-report/551/2> accessed 1 August 2023.

ranging from criminal sanctions for child abuse, orders imposed in civil litigation, to demands of administrative authorities in consumer or medical law.

As explained by AG Szpunar, according to the preparatory works relating to the ECD,[19] 'the limitation of liability in question extends, horizontally, to all forms of liability for unlawful acts of any kind, and thus to liability under criminal law, administrative law, and civil law, and also to direct liability and secondary liability for acts committed by third parties'.[20] Under the DSA, 'illegality' is defined with reference to the national and EU legal orders. In utilising the term 'liability', the DSA encompasses any legal consequences that national law imposes on providers if such consequences are in any way triggered by their users' behaviour when using their services. While the users' behaviour is abstracted into the notion of 'information', since every move in the digital world produces information, the scope effectively covers any traces left by interactions between users and relevant providers of digital services.

The only form of liability specifically singled out for a different treatment is targeted injunctions. As noted by AG Spzunar, the ECD 'makes a distinction between actions for damages and injunctions which must be taken into account when it comes to identifying the delimitation of liability prescribed in that provision'.[21] The CJEU confirms the special status of the injunctions.[22] This means that the exempted liability in Articles 4–6 DSA covers injunctions; however, *some* of them are, in turn, permitted by so-called injunction clauses (Articles 4(3), 5(2), and 6(4) DSA). According to the CJEU:

> [a liability exemption] of the directive does not preclude the person harmed by that infringement from *seeking before a national authority or court* to have the service provider prevented from allowing that infringement to continue.[23]

As explained in Chapters 5 and 8, this means that only orders of *authorities* are permitted to impose specific obligations on the providers subject to liability exemptions. Thus, for instance, a national law allowing non-state actors to formulate a binding request would be trying to impose liability that is exempted; such national rules must be set aside as violating Articles 4–6 DSA.

A special case of liability is pre-trial compensation and trial costs. The CJEU clearly held in *McFadden* that such compensation, as an ancillary claim connected with enforcing the main pecuniary claims such as damages, is limited by liability exemptions. As explained by the CJEU,[24] 'to be well founded, such an ancillary claim requires that the principal claim is also well founded'.

[19] 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.

[20] Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:170, Opinion of AG Szpunar, para 64; also Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2021:613, Opinion of *AG Øe*.

[21] *McFadden (Opinion of AG Szpunar)* (n 20) para 70.

[22] Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:689, para 77.

[23] *McFadden (Opinion of AG Szpunar)* (n 20) paras 68–69.

[24] *McFadden* (n 22), para 75 (in the context of mere conduit exemption).

However, the CJEU held the opposite to be the case for injunctions. AG Szpunar argued that the liability exemptions should also cover 'any other pecuniary claim that entails a finding of liability for copyright infringement with respect to the information transmitted, such as a claim for the reimbursement of pre-litigation costs or court costs'.[25] The Court, probably driven by deference to national procedural rules, ruled the opposite—namely that pre-trial compensation and trial costs associated with permitted injunctions are not precluded by the provision. It held that the mere conduit liability exemption 'does not prevent that same person from claiming the reimbursement of the costs of giving formal notice and court costs incurred in a claim [before a national authority or court to have the service provider prevented from allowing that infringement to continue]'.[26] It remains unclear how broadly this allowance for pre-trial and trial costs of seeking permitted injunctions is to be interpreted. Does it only apply to the situation when authorities get involved? Or does it apply to any substantive claim for injunctive relief regardless of whether authorities have reviewed the claim?[27] In my view, and in line with injunction clauses, such a reading should be limited to cases whereby injunctions were sought before the authorities. Otherwise, the argument about protecting procedural autonomy holds barely any water.

6.2.4 The neutrality condition

The goal of liability exemptions is to limit the liability for non-editorial content originating from users and not limit the liability for the platform's own editorial content. Thus, as explained above, a newspapers liability might be limited for comments, but not for its journalism. While in theory, the line between the two seems clear, in practice, it is becoming a heavily contested one with the growing integration of user-generated content into services. In addition, if users are acting on the instruction of the providers themselves, such content is not non-editorial either. For instance, a comment posted by an employee or contractor in the discussion forum remains editorial. The liability exemption system, thus, must be able to define the criteria for when users' content is not users anymore.

In its first Grand Chamber judgment, *Google France*, the CJEU developed a doctrine of neutrality limiting the applicability of all three liability exemptions in situations when the providers act beyond their role as 'intermediaries'.[28] Invoking a recital, it held that the hosting safe harbour only applies to a provider whose position is 'neutral'

[25] *McFadden (Opinion of AG Szpunar)* (n 20) para 74.
[26] *McFadden* (n 22) paras 77–78.
[27] On the risks of this interpretation Martin Husovec, 'Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours' (2017) 12(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 115.
[28] Cases such as Joined Cases C-236/08–C-238/08 *Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2010:159 (*Google France*); Case C-324/09 *L'Oréal SA and others v eBay International AG and others* ECLI:EU:C:2011:474; Case C-521/17 *Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta* ECLI:EU:C:2018:639; Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503.

in relation to user-uploaded content.[29] The test is whether the provider's 'conduct is purely technical, automatic and passive, which implies that that provider does not know or control the data which it stores'.[30] Any disqualifying active intervention gives the provider 'knowledge of and control over the content'.[31] However, the disqualification applies only to specific content with respect to which the provider did not behave neutrally, and not all the remaining content on the service.[32]

Subsequent case law tried to determine what constitutes a disqualifying level of 'knowledge or control'—most of the time, without much success in clarifying the issue. In the two Grand Chamber cases, *L'Oréal v eBay* (2011) and *YouTube and Cyando* (2021), the Court hardly advanced a unified test of neutrality.

The test used by the Court is capable of solving easy cases, such as whether newspapers are exempt from their liability for their own articles.[33] In *Papasavvas*, the CJEU applied the test[34] and held that 'since a newspaper publishing company which posts an online version of a newspaper on its website has, in principle, knowledge about the information which it posts and exercises control over that information, it cannot be considered to be an "intermediary service provider" within the meaning of Articles 12 to 14 of Directive 2000/31'.[35] The Court, however, never explained why this is the case.

This distinction was primarily important for hosting services, even though it applies equally to mere conduits and caching services. The nebulous case law of the CJEU led to numerous disputes about the concept of passivity. It led to cases before the European Court of Human Rights, such as *Delfi v Estonia* and *Sanchez v France*, that arguably should never have ended up there on a proper reading of the EU law.[36] The *eBay* ruling was particularly unhelpful in bringing clarity to the issue.[37] It led to widespread speculation as to whether 'presentation optimisation' is sufficient to lead to a loss of neutrality.

The CJEU case law led some Member States courts to conclude that many providers lost their neutrality and gave ammunition to some industries that viewed the relevant case law as suggesting that mere *technical control* of information already disqualifies them from EU protections. This expansive interpretation of passivity greatly influenced

[29] See extensively on the history of this: Martin Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (Cambridge University Press 2017); Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Edward Elgar Publishing 2020).

[30] *Google France* (n 28) para 114; *eBay* (n 28).

[31] *YouTube and Cyando* (n 28) para 109.

[32] *Google France* (n 28) paras 109, 120 ('those data'); *eBay* (n 28) para 113 ('those data').

[33] *Papasavvas* (n 13) para 45.

[34] ibid 44.

[35] ibid 45. The Austrian Supreme Court held in 2016 that an owner of a page can qualify as a hosting provider (Case No 6Ob244/16z).

[36] In *Delfi AS v Estonia* App no 64569/09 (ECtHR, 16 June 2015), the Estonian courts erroneously ruled that a newspaper hosting comments of others is not a passive host. In *Sanchez v France* App no 45581/15 (ECtHR [GC], 15 May 2023), the French courts did not even consider that the administrator of a page on social media could be a hosting provider vis-à-vis comments posted by users and thus shielded from liability for them.

[37] *eBay* (n 28) para 116. What seemed to have been overlooked by some national courts was the fact that in the *eBay* case, *eBay* itself actively promoted some advertisements outside of its services on websites such as Google or MSN and assisted with optimisation within its website. eBay chose the relevant keywords to advertise and paid for the advertising. Thus, optimisation expressed active contribution by employees of *eBay*: see *eBay* (n 28) para 31; *L'Oreal SA v Ebay International AG* [2009] EWHC 1094 (Ch) [26], [52] (High Court of England and Wales, Chancery Division).

the 2016–19 EU copyright debate. The European Commission's copyright unit even used the terms from the case law to justify its expansion of the 'communication to the public' right in 2016.[38] The neutrality test was thus bound to influence the DSA debate.

In December 2019, the newspapers reported that, according to the Commission, 'concepts such as 'active' or 'passive' hosts, linked by the Court to the notion of 'optimising content', appear outdated in light of today's services'.[39] Public consultation,[40] targeted interviews with judges,[41] and studies outsourced by the Commission[42] in preparation for the DSA concluded that the 'active/passive dichotomy' was unclear and needed further clarifications. In the Impact Assessment, the Commission stated that:

> The fact that there is no such thing as an 'active host', but that a provider might play an active role regarding some listings, but not others (for instance because it presents it or recommends it in a special manner) does not lead to the necessary legal certainty to provide legal intermediation services without risking claims for damages or even criminal liability. Many automatic activities, such as tagging, indexing, providing search functionalities, or selecting content are today's necessary features to provide user-friendly services with the desired look-and-feel, and are absolutely necessary to navigate among an endless amount of content, and should not be considered as 'smoking gun' for such an 'active role'.[43]

Eventually, however, in its 2020 proposal for the DSA, the Commission did not explicitly touch the concept. It only reworded the relevant ECD recitals that originally gave birth to the doctrine. The text of Recital 42 ECD was modified into Recital 18 DSA, which states the following:

> The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of the intermediary service itself, including where the information has been developed under the editorial responsibility of that provider.

[38] Commission, 'Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market (CDSM Directive)' COM/2016/0593 final, Rec 38 ('In respect of Article 14, it is necessary to verify whether the service provider plays an active role, including by optimising the presentation of the uploaded works or subject-matter or promoting them, irrespective of the nature of the means used therefor').

[39] Alexander Fanta and Rudl Tomas, 'Leaked Document: EU Commission Mulls New Law to Regulate Online Platforms' (*Netzpolitik*, 16 July 2019) <https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/> accessed 1 August 2023.

[40] Commission, 'SWD(2020) 348 Final' (n 4) annex 2.

[41] ibid.

[42] Sebastian Schwemer, Tobias Mahler, and Håkon Styri, *Legal Analysis of the Intermediary Service Providers of Non-Hosting Nature: Final Report* (EU Publications Office 2020) 32.

[43] Commission, 'SWD(2020) 348 Final' (n 4) annex 9.

Recital 18 thus consolidated the test—though still not clarified it. It repeats the criteria from the case law of the CJEU, such as knowledge or control, but it also links them to 'editorial responsibility'—a term that previously was not used by the ECD.[44] The European Commission was probably modest because AG Øe's Opinion in *YouTube and Cyando* dispelled some of the biggest misunderstandings about the concept.[45] It was only during the legislative process that the Court arguably tried to address the confusion introduced in its previous Grand Chamber ruling in *eBay*. However, although it did solve some issues, the Court still hardly clarified the concept. The *YouTube and Cyando* decision de facto held that the most common activities of modern digital services—algorithmic categorisation, personalisation, ranking or provision of search—do not disqualify providers from neutrality and do not rob them of protections.

Indeed, the *YouTube and Cyando* decision of the Grand Chamber provides the most elaborate application of the neutrality condition in the pre-DSA context. However, the judgment itself is not among the clearest because it interchangeably shifts between three different issues: a) the neutrality of hosting providers, b) the criteria for communication to the public, and c) the standard of specific knowledge required to strip hosting providers of their exemption. The Court's reasoning is construed by arguing first that no hosting provider that fulfils the criteria for communication to the public can be neutral.[46] Thus, whatever qualifies someone as communicating their users' content to the public must also disqualify him from neutrality. Second, the Court explains what activities do not constitute 'specific knowledge', and thus knowledge that can strip hosting providers from the liability exemption. Since, as I have argued above, the standard for neutrality must be stricter, logically, whatever is not sufficient to confer specific knowledge can neither confer 'specific knowledge of' for neutrality purposes.

With this caveat, the ruling confirms several important issues. The Court held that algorithmic categorisation, personalisation, ranking or provision of search do not confer specific knowledge.[47] It is not sufficient that the provider has abstract knowledge (meaning general awareness) that his service carries some infringing content.[48] However, if it is true that neutrality's 'knowledge of' must be more stringent, then this clearly also means that these same activities cannot disqualify from neutrality. It also clarified that the installation of content monitoring tools that help to uncover infringing content does not constitute an active intervention which disqualifies them from neutrality.[49] In the DSA, these findings are now incorporated into Recital 22

[44] In DMCA legislative history, the editorial decisions of providers were being discussed already: 'HR Rep No 105–551 Part 2 (1998)' (n 18) at 51 ('The term "selection of the material" … means the editorial function of determining what material to send, or the specific sources of material to place on-line [eg, a radio station], rather than "an automatic technical process" of responding to a command or request, such as one from a user, an Internet location tool, or another network').

[45] *YouTube and Cyando (Opinion of AG Øe)* (n 18) paras 158, 161: 'eBay sometimes promotes some offers on the Internet itself outside its business'.

[46] *YouTube and Cyando* (n 28) paras 107–08.

[47] ibid para 114.

[48] ibid para 111.

[49] ibid para 109.

as clarifications of when 'specific knowledge' required by the hosting exemption is missing and Article 7 DSA concerning voluntary own-initiative investigations and legal compliance.

The CJEU in its discussion builds on AG Øe's Opinion which defined the neutrality test as follows:

> I understand the Court's case-law to mean that a provider plays an 'active role' of such a kind as to give it 'knowledge of, or control over', the data which it stores at the request of users of its service where it does not simply engage in the processing of that information, which is neutral vis-à-vis its content, but where, by the nature of its activity, it is deemed to acquire intellectual control of that content. That is the case if the provider selects the stored information, if it is actively involved in the content of that information in some other way or if it presents that information to the public in such a way that it appears to be its own. In those circumstances, the provider goes outside of the role of an intermediary for information provided by users of its service: it appropriates that information.[50]

In AG Øe's view, the 'involvement' must concern 'intellectual control', which results in the 'appropriation' of information. This, in my view, maps well to the language of the DSA and my conceptualisation below. In fact, the above paragraph is followed by *AG*'s citation to my prior work[51] that discussed the German doctrines of adopted content and why the neutrality test partly serves to demarcate what is still third parties' and already providers' content.

In sum, the *YouTube and Cyando* judgment, informed by AG Øe's Opinion, improves our understanding of neutrality. It makes it clear that neutrality cannot be lost by the omnipresent technical functionalities of the interactive web but only by interventions that get the providers 'too involved' in the content of their users. The judgment also clarifies the underlying policy rationale, which is to draw the line when providers either instruct the production of content or appropriate it so much that they must gain editorial responsibility. Despite all these new insights, the judicial test for neutrality remains underdeveloped.

Even the DSA's new text introduces new hints but cannot deliver a test. According to Folkert Wilman of the Commission's Legal Service:

> … there seems to be a subtle development. In particular, there is no reference to a requirement of passivity on the part of the service provider – its role may therefore be active to a certain extent, as long as it does not lead to knowledge or control in the sense just mentioned. In this manner the DSA deviates somewhat from the E-Commerce Directive, which contained such a reference to passivity.[52]

[50] *YouTube and Cyando (Opinion of AG Øe)* (n 18) para 152.
[51] ibid fnn 52 and 142, citing Husovec (n 29) 55–57.
[52] Folkert Wilman, 'The Digital Services Act (DSA) – An Overview' (2022) 6 <https://www.ssrn.com/abstract=4304586> accessed 1 August 2023.

Recital 22 concerning conduits and caching speaks of not 'alter[ing] the integrity of the information' as opposed to 'manipulations of a technical nature'. The conduit exemption in Article 4 speaks of *not* initiating the transmission, selecting its receivers, and selecting or modifying the information contained. Caching exemption in Article 5 speaks of *not* modifying information and complying with some industry standards. Hosting exemptions in Article 6 speaks of *not* acting under the authority or the control of the provider and *not* creating the impression that the online platform provides information.

Recital 18 consolidates the test to 'play[ing] an active role of such a kind as to give it knowledge of, or control over, that information'. Knowledge and control are thus two different mutually non-exclusive criteria. Newspapers publishing articles by freelance journalists have both 'knowledge of' their articles and 'control over' them. Since editors can influence the content of those articles, and they might have instructed their authors, the conclusion seems inescapable. However, how about an app store that publishes its guidance for app developers and screens apps before their distribution? Does quality control confer on the app store 'knowledge of' or 'control over' the apps?

In my view, different active interventions could be depicted on a spectrum like the one below. Sprinkled around the DSA are numerous references to neutrality. Looking at the universe of possibilities, two elements of the test can be translated as 'control over meaning' and 'knowledge by participation'. Logically, the standard for 'knowledge of', triggering loss of neutrality, must be more stringent than the standard of actual knowledge triggering loss of hosting exemption. Otherwise, the former would be superfluous, and there would be no difference between the various exemptions.[53] On the contrary, the opposite is visible in that each liability exemption has its own set of qualifiers that further flesh out what constitutes active interventions (eg mere conduit cannot modify transmitted information but hosting services can to some extent). I will argue that these specific active interventions reveal what type of control Recital 18 is about. In my view, the DSA and case law are converging on the notion that 'control over' means control over the *meaning* of information, ie control over *who* says *what* (see Figure 6.2).

6.2.4.1 Editorial control

Newspapers control the meaning of information. By editorial control, they influence what journalists write. Hence, they are not neutral with respect to journalistic articles. Blogs, in contrast, do not influence what bloggers publish. Even if they pre-approve content, they do not edit submitted blogs. However, if a newspaper running a blog section edits a blog article and republishes it with its other journalistic articles, its relationship to that specific article is no longer neutral. It does not matter that the article was

[53] The ruling in *McFadden* rejected the knowledge requirement for all liability exemptions.

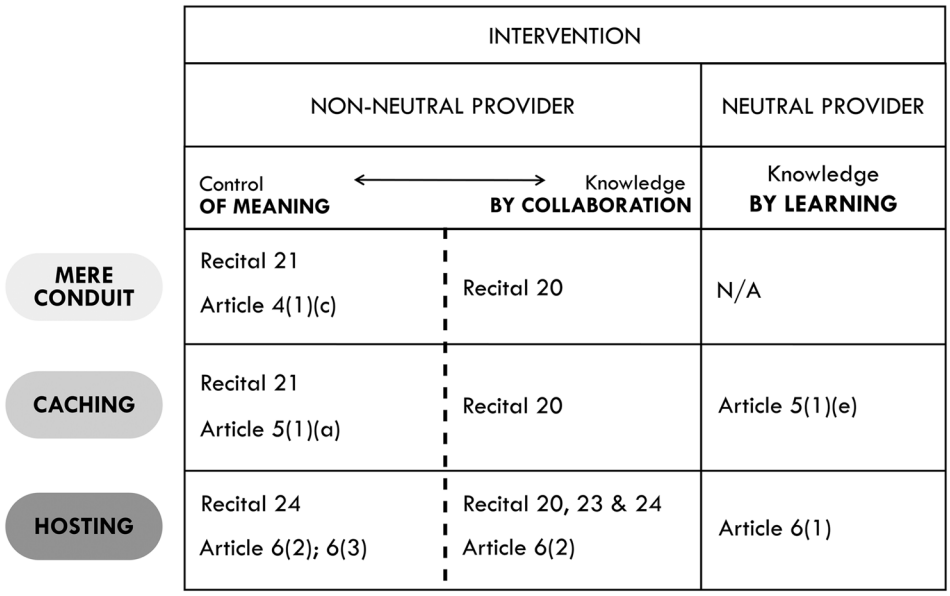

Figure 6.2 Neutrality of services

not originally developed under editorial responsibility. The same conclusion should apply if the newspaper did not edit the article but would simply present it to readers as its own newspaper content. This hypothetical shows that control over the meaning of information covers situations when providers influence *what* is being published by users, as well as when they change *who* is publishing it.

Conduit and caching exemptions have specific language in the exemptions themselves supporting such reading of what constitutes neutrality of control over information (eg Articles 4(1)(c), 5(1)(a), etc). As noted by Recital 21, '[neutrality] should not be understood to cover manipulations of a technical nature which take place in the course of the transmission or access, as long as those manipulations do not alter the integrity of the information transmitted or to which access is provided'. Thus, 'control over meaning' does not extend to *mechanical manipulations* that do not influence the information's integrity. However, who expresses the information plays a part in determining integrity if such information is published. The hosting exemption now clarifies this with a new paragraph specifically addressing the situation when users' content is presented as providers' own (Article 6(3)). In such cases, providers do not change what is said, they only change who says it. If reasonable readers read information as originating from the provider, one can question providers' neutrality, too. If providers hide the origins of information to create the impression that it is of their own provenance, they accept editorial responsibility. Therefore, the bots that rely on user-generated content without properly attributing it cannot be treated as neutral providers even if they meet other criteria.

'Knowledge of', in contrast, covers situations where a user acts as a proxy. In these cases, the provider usually instructs a user to do something. A typical example of this

is the CJEU case of '*The Pirate Bay*'.[54] The provider here intentionally instructed by inducing its users to violate the law by uploading some material. As noted by Recital 23, such a user 'is acting under the authority or the control of the provider'. The provider instructing thus clearly cannot be neutral as he wishes the outcome to materialise. The hosting exemption specifically reflects this in its liability exemptions (Article 6(2)).

Both the ECD and the DSA anticipate this sort of accessorial liability: the ECD excluded from the liability exemption those cases where the provider exercises authority or control over the content provider (Article 14(2) ECD, for hosting services) or '*deliberately* collaborates with one of the recipients of his service to undertake illegal acts' (Recital 44 ECD, initially for mere conduits and caching services). The DSA's Recital 20 reiterates and reinforces the language previously used by ECD as follows:

> Where a provider of intermediary services deliberately collaborates with a recipient of the services in order to undertake illegal activities, the services should not be deemed to have been provided neutrally and the provider should therefore not be able to benefit from the exemptions from liability provided for in this Regulation. This should be the case, for instance, where the provider offers its service with the main purpose of facilitating illegal activities, for example by making explicit that its purpose is to facilitate illegal activities or that its services are suited for that purpose. The fact alone that a service offers encrypted transmissions or any other system that makes the identification of the user impossible should not in itself qualify as facilitating illegal activities.

The difficult question is to decide what level of knowledge of the illegal acts of the user is necessary. As explained above, logically, the standard for 'knowledge of' triggering loss of neutrality must be more stringent than the standard of actual knowledge triggering loss of hosting exemption. Thus, the mental element of the provider must go beyond simply *knowing* that a user will commit specific illegal actions. The provider must be somehow implicated in the users' actions. One of the obvious ways would be to conceptualise 'knowledge of' as 'knowledge of participation', borrowed from criminal law. In most legal systems, providers could become accessors when they *intentionally* participate in the acts of others.[55] Arguably, this is what the word 'deliberately' suggests.

6.2.4.2 A possible test for neutrality

Thus, the neutrality test could be formulated as follows: *did the platform exercise control over the meaning of the user's content, or does it have knowledge of its own deliberate participation in the acts of users?*

Two parts of the test are not mutually exclusive (eg newspapers deliberately participate in publishing stories of their freelance journalists and have control over the

[54] Case C-610/15 *Stichting Brein v Ziggo BV and XS4All Internet BV* ECLI:EU:C:2017:456 (*The Pirate Bay* [CJEU]).

[55] For a comparative overview of secondary liability, Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Wolters Kluwer 2017). For an overview of the English situation, Pey Woan Lee, 'Accessory Liability in Tort and Equity' (2015) 27 Singapore Academy of Law Journal 851.

substance of published articles). However, many situations would fall under one of the two subparts of the test. Let me offer some examples:

- App stores controlling the quality of submitted apps that undoubtedly obtain knowledge of the apps they distribute (though not necessarily of illegality of those apps) would remain neutral unless they deliberately participate in the app owners' specific wrongs, such as consumer fraud.
- A newspaper routinely pre-approving comments by users caught by its hate speech detection tool would preserve neutrality even when they sometimes obtain knowledge of circumstances. They could fail to act upon such knowledge by failing to investigate them but that would strip them of the liability exemption for a different reason.
- A hotel that specifically advertises its wi-fi connectivity as a good means to 'not get caught by law enforcement' could be viewed as losing neutrality for deliberately participating in the wrongs of its clients found to use the connection to commit some crimes.
- A price-comparison site that compiled product descriptions from various submissions of sellers by algorithmically evaluating their quality and then collaging various high-quality pieces into one text would lose neutrality because it produces new content with new meaning.
- An online marketplace that hides the identity of its sellers so that users cannot distinguish if they are buying from the provider or someone else would disqualify from neutrality because it gains control over the substance of the content by substituting itself as the expected producer of information.
- A video-sharing platform that automatically blurs potential depictions of violence would not be disqualified from neutrality because its interventions are merely mechanical and do not alter the meaning.
- A social network that attaches warning to posts of their users would not lose neutrality because the additional information does not alter the meaning of the commented information.
- A video-sharing service that ranks and recommends the content of its users via an algorithm would not lose neutrality because such recommendation does not change the meaning of the information ranked or recommended.

The difference between the price-comparison website and the video-sharing platform is that while both are involved in the substance of content, the video-sharing platform does not alter what is said. In contrast, the price-comparison website only uses users' information to produce new content with new meanings. The online marketplace does not change what is being said, as it preserves the originally submitted content, but alters who is saying it in the readers' perception.

Intervening in the meaning of the users' content thus has two dimensions: *who* says *what*. If the platform influences *what* is said by meaningfully intervening in drafting the provided information, algorithmically or not, it exercises intellectual control. Similarly,

if the platform changes *who* says something by presenting the provided content as its own and concealing its true authorship, it alters the meaning of the underlying information. The content now reads like a statement from the platform, not that of a third party. This last situation of 'adopted content' is now explicitly recognised by Article 6(3) DSA.[56]

In the assessment of 'adopted content', it is less important to consider what *tools* are used rather than what the *outcome* is for the reader. If a platform appropriates third-party content by presenting it as its own, it does not matter if this integration results from algorithms or human actions. In both cases, the meaning of the information changes.[57] Similarly, while a platform employee's suggestion as to what to include would qualify as an active intervention, the same can be said of automated tools that force the choice of the original author of the content. For instance, if an app provides the choices of background music to users of video-sharing platforms, it is unlikely to be able to claim a liability exemption for the inclusion of such music. At the same time, if the elements that are not the result of pre-selection can be separated, the liability exemption could continue to apply. Thus, a defamatory video that carries a piece of pre-approved music does not disqualify the provider from protection vis-à-vis the defamatory message. The video could be said to contain two different pieces of information despite being presented together as sound and image.

The 'control of the meaning', or as put by AG Øe, 'intellectual control', must be distinguished from purely *mechanical contributions*. When a platform changes the content's font or format, there is no intervention on who says what—only the presentation of the information changes. This also follows from the recitals, which stress that modification for mere conduits and caching 'should not be understood to cover manipulations of a technical nature which take place in the course of the transmission, as such manipulations do not alter the integrity of the information transmitted'.[58] The same is true for hosting, for instance, when the platform provides an automated translation of the text. However, if such translation mistakenly alters the meaning, the platform itself arguably changes what is said and thus exposes itself to liability.[59] The extent of acceptable mechanical contribution may differ based on the proximity of providers to their content. This is already implied in the different requirements found across the liability exemptions.

The above distinctions explain why categorisation, personalisation or ranking in the search results do not constitute disqualifying active interventions. They do not alter who says what; they only influence the delivery of the information. They assist the reader when receiving the information provided by the original author, but they do

[56] See also *YouTube and Cyando (Opinion of AG Øe)* (n 18) para 152.

[57] Consider a situation of a news portal that integrates parts of user comments into the content of articles without the author being obvious to the reader. In that case, the content would change, as the originator of the information would change from the reader's point of view. The reader would consider this is information is voiced by a news portal.

[58] DSA, Rec 21; ECD, Rec 43.

[59] This must be distinguished from when users utilise plug-ins. In these cases, translation is done by readers or users and not by platforms.

Table 6.1 Situations leading to the loss of neutrality

'Control over' meaning	**'Knowledge of' own deliberate participation**
A provider co-determining user's content	A provider instructs the user's wrongs
A provider presenting user's content as the provider's own	A user acting under a provider's control or jointly collaborating

not interfere with what the author communicates. This is also true when an algorithm selects and subsequently displays only some of the content initially provided, so long as the author of such content is clearly designated to the reader.

This reading of neutrality thus presents the providers with a clear choice. If providers wish to integrate content heavily in their offering by instructing their users, redesigning their content, or concealing its origin, they can do so, but at the expense of losing the liability exemptions. Policy-wise, the resulting content shall then be regarded as editorial regardless of the means used to produce it or the fact that the finished product's ingredients come from user-generated content.

Table 6.1 summarises the typical examples of active interventions.

6.2.5 Provider's own investigations

The DSA's liability chapter has introduced a new provision meant to provide interpretive guidance. Article 7 does not introduce a new liability exemption; however, it informs how to interpret various components of liability exemptions, and the prohibition of general monitoring obligations.

According to Article 7 DSA, entitled '[v]oluntary own-initiative investigations and legal compliance', the following conduct must be encouraged:

> Providers of intermediary services shall not be deemed ineligible for the exemptions from liability referred to in Articles 4, 5 and 6 solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation.

The provision addresses the common concern that the voluntary actions of providers can cost them liability exemptions either because they lose the status of neutrality or gain knowledge as hosting providers. The CJEU has in *YouTube and Cyando* before the DSA's adoption that the same followed already from the previous framework: 'the fact … that the operator of a video-sharing platform, such as YouTube, implements technological measures aimed at detecting … content which may infringe copyright,

does not mean that, by doing so, that operator plays an active role giving it knowledge of and control over the content of those videos'.[60] Article 7 introduces some more explicit language.

At this point, the added value of the provision is uncertain. On the one hand, it clearly can inform other provisions and their interpretation by articulating that desirable enforcement efforts should not be punished, and thus disincentivised, by increased uncertainty about providers' liability. In this sense, the provision draws inspiration from section 230(c) Communications Decency Act[61] that tried to give comfort to 'good Samaritans' who, following the *Prodigy* ruling,[62] were suddenly exposed to a worse legal situation if they did more to moderate the content of their users. However, Article 7 is a very different animal in a very different zoo. The DSA does not grant any legal immunity from liability for good faith content moderation actions. It only makes sure that existing liability exemptions are preserved. Thus, potential disincentives in the form of any liability to affected users remain unaddressed.

Some scholars like Kuczerawy worry that Article 7 might incentivise only more enforcement and thus more content removals because it does not provide well-rounded immunity.[63] I am less sure. Because the crucial counter-incentive—potential legal consequences for over-removal vis-à-vis a user—is not included in the immunity, the situation would appear the same as pre-DSA. However, given that the DSA increases incentives against over-removal elsewhere (see Chapters 10–11), I do not see deterioration of the incentive situation. However, I am equally unsure whether Article 7 will substantially change the case law on any related points: neutrality or knowledge.

Firstly, after *YouTube and Cyando*, neutrality clearly cannot be lost by simply doing more than notice and takedown. Post-DSA, many online platforms will have to do substantially more; thus, using the DSA-imposed measures on them to strip them of liability exemptions would be internally inconsistent. For very large online platforms (VLOPs), due to their big risk mitigation obligation under Article 35, there is hardly any space to say that some measures are still truly 'voluntary'. Second, post *YouTube and Cyando*, the case law is now also clear that the diligence expected of providers is limited to assessment 'without a detailed legal examination, that that communication is illegal and that removing that content is compatible with freedom of expression'.[64] Thus, even where circumstances arise during the carrying out of voluntary measures that show some indications of illegal behaviour, the indications must be very strong —basically limited to obviousness—that some behaviour is illegal. In my view, the likelihood of randomly bumping into specific knowledge about illegality without realising it is, very low.

[60] *YouTube and Cyando* (n 28) para 109.
[61] 47 US Code § 230(c).
[62] *Stratton Oakmont Inc v Prodigy Services Co* 23 Media L Rep 1794 (NY Sup Ct 1995).
[63] Aleksandra Kuczerawy, 'The Good Samaritan That Wasn't: Voluntary Monitoring Under the (draft) Digital Services Act' (*Verfassungsblog*, 12 January 2021) <https://verfassungsblog.de/good-samaritan-dsa/> accessed 1 August 2023.
[64] *YouTube and Cyando* (n 28) para 116.

6.2.6 Economic nature of services

The 'Digital Services Act' does not refer to 'digital services' in its articles. Instead, the DSA speaks about 'intermediary services'—services that store or give access to people's communications. The DSA does not regulate editorial services, such as newspapers or streaming. Looking at the digital ecosystem, 'intermediary services' are the most important types of digital services. Among the top 50 visited websites on the internet globally, the majority rely on users—ie other people, like you and I—to generate the content.[65] Thus, while the DSA is mostly about user-generated content, or user-to-user communication tools, because of the nature of such content the DSA is crafted broadly enough to capture most of the digital ecosystem (see Chapter 1).

But one limitation of the DSA is perhaps more consequential—ie a limitation to services of an economic nature.

Article 2 limits its scope to 'intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment'. Article 3(f) defines 'intermediary service' as one of the following information society services: (i) a 'mere conduit' service; (ii) a 'caching' service, or (iii) a 'hosting' service. Finally, Article 3(a) defines 'information society services' as a 'service' as defined in Article 1(1), point (b), EU Directive 2015/1535. According to Article 1(2) of EU Directive 2015/1535, an 'information society service covers any service normally provided for remuneration, by electronic means and at the individual request of a recipient of services'.[66]

So, in a nutshell, to be in the scope of the DSA, a firm needs to provide an intermediary service, which in turn needs to be an information society service, which in turn needs to be a service. And what is a service? Article 57 TFEU establishes a very open definition: 'Services shall be considered to be "services" within the meaning of the Treaties where they are normally provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement for goods, capital and persons.' Therefore, the main characteristic of a service is to be 'normally provided for remuneration'—a tricky condition in the context of ubiquitous and freely available online tools that might not always be at first 'normally provided for remuneration'.

In 2000, the ECD already had to confront this question. Recital 18 ECD clarifies that 'information society services are not solely restricted to services giving rise to online 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 online

[65] The list at 'List of Most Visited Websites', *Wikipedia* (2023) <https://en.wikipedia.org/w/index.php?title=List_of_most_visited_websites&oldid=1168840226> accessed 8 August 2023.

[66] European Parliament and Council Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and rules on Information Society services (2015) OJ L241/1, codifying: European Parliament and of the Council Directive 98/48/EC of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations (1998) OJ L217/18.

information or commercial communications, or those providing tools allowing for search, access and retrieval of data'. The CJEU has clarified that the concept of 'normally provided for remuneration' does not have to entail reliance on fees in the provider's business model. According to the CJEU, '[t]he remuneration of a service supplied by a service provider within the course of its economic activity does not require the service to be paid for by those for whom it is performed'.[67] Even free-of-charge services whose business models are based on advertising or other business models,[68] such as the resale of data or analytics, can qualify as 'normally provided for remuneration'.

In the context of multi-sided platforms, for instance, the fact that the user receives the service for free does not exclude it from constituting an economic activity, as other recipients of the service (such as advertisers or traders) will remunerate the service. In any event, it requires exercising an economic activity or being provided in the context of economic activity. In *Papasavvas*, the Court linked the concept to primary law when it held that 'interpretation corresponds to that of the concept of 'services' within the meaning of Article 57 TFEU, which also does not require the service to be paid for by those for whom it is performed'.[69] The Court then argued that advertising undoubtedly turns the activity into services.[70] In *McFadden*, the CJEU established that offering access to a WiFi hotspot for free constituted a service, 'where the activity is performed by the service provider in question for the purposes of advertising the goods sold, or services supplied by that service provider'.[71] In other words, if the provider has some business motive, there is no doubt that it will qualify under the condition.[72]

However, if it does not, and thus an economic motive is missing in their case, it depends on what interpretation is given to the term. The case law to date did not fully clarify whether the test is 'objective'—ie a service is capable of being provided for remuneration, or is usually provided in such way by others—or 'subjective'—ie a service is being provided for remuneration in this specific case.

I think that the objective test is more appropriate. With the subjective test, two persons in the same position can be treated differently only because they rely on different motives when doing the same thing. It would mean that non-profit entities or public services do not enjoy protections afforded to large corporations and limit the availability of enforcement tools in the DSA against such entities. Adopting the subjective interpretation would mean that national law can decide whether it wishes to extend the application of liability exemptions per analogy to such 'non-economic' services. This, in my view, would seriously compromise the harmonising effect and the effectiveness of the DSA. Digital offerings could escape DSA obligations by framing their activities as merely charitable or non-profit projects.

[67] *McFadden* (n 22) para 41.
[68] *McFadden* (n 22) para 42 ('where the performance of a service free of charge is provided by a service provider for the purposes of advertising the goods sold and services provided by that service provider, since the cost of that activity is incorporated into the price of those goods or services').
[69] *Papasavvas* (n 13) para 29.
[70] ibid para 30.
[71] *McFadden* (n 22) para 41.
[72] For a CJEU case supporting this reading, see Case C-339/15 *Vanderborght* ECLI:EU:C:2017:335.

The danger is real. The Slovak Supreme Court, applying the *McFadden* ruling,[73] recently opined that when a non-profit organisation operating a local news website hosts comments, it does not engage in economic activity.[74] As a result, the organisation does not benefit from the liability exemptions, and going forward, equally would not be subject to the due diligence rules of the DSA. The Member States can decide to align such situations with the DSA as they see fit. However, for liability exemptions, the human rights law can de facto impose an obligation to extend comparable regimes to non-profit actors.[75]

While so far, we only have very few cases where providers would try to escape the definition of services, this might change under the DSA. Providers themselves have favoured and profited from wide interpretation. Under the pre-DSA legal landscape, 'being a service' meant benefitting from the treaty-based free movement of services; being an information society service means benefitting from the country-of-origin principle under the ECD; being an intermediary service means benefitting from a liability exemption. There were many benefits and few obligations. These changes under the post-DSA landscape create incentives to treat economic character as a loophole.

To close such a loophole, if a service can be turned into a business, regardless of whether it has already been, it should be viewed as a 'service'. Thus, a non-profit service like Wikipedia, supported by donations, can always decide to sell insights,[76] should equally profit from liability exemptions, and be bound by DSA obligations. Its legal regime should not be dependent on the funding model of the service. This is in line with the traditional interpretation of the concept of 'service', which has been very broad.[77] Only such an objective reading assures that some players do not try to game the system by carefully timing their for-profit operations to avoid due diligence obligations.

This reading finds support in *European Commission v Hungary*, where the CJEU held that:

> The decisive factor which brings an activity within the ambit of the FEU Treaty provisions on the freedom to provide services and, accordingly, of those relating to the freedom of establishment, is its economic character, that is to say, *the activity must not be provided for nothing*. By contrast, contrary to what is maintained by the Hungarian Government, *there is no need in that regard for the person providing the service to be seeking to make a profit …* [78]

[73] *McFadden* (n 22).
[74] The Slovak Supreme Court (2022) Case No 9Cdo/78/2021, paras 34–37.
[75] Ch 3.
[76] Sarah Perez, 'Google and the Internet Archive Are the First Customers to Gain Commercial Access to Wikipedia Content' (*TechCrunch*, 29 June 2022) <https://techcrunch.com/2022/06/29/google-and-the-internet-archive-are-the-first-customers-to-pay-for-commercial-access-to-wikipedia-content/> accessed 1 August 2023.
[77] Lilian Edwards (ed), *The New Legal Framework for E-Commerce in Europe* (Hart 2005) 95.
[78] Case C-179/14 *European Commission v Hungary* ECLI:EU:C:2016:108, para 154.

Thus, whether an entity is seeking immediate profit is irrelevant. If it builds a digital service which generates value for others, it is not provided for nothing, irrespective of whether that value is converted into money.

A separate question concerns state-run services, such as domain name authorities for top-level domain names ('.fi' for Finland), run by the state in some countries. One can borrow from the CJEU's competition case law to consider whether these services qualify as a service. Here, the CJEU held that 'an undertaking is any entity engaged in an economic activity, irrespective of its legal status and the way in which it is financed'.[79] Any activity 'consisting in offering goods and services on a given market is an economic activity'.[80] Thus, the state may act as an undertaking, unless its activities 'fall within the exercise of public powers are not of an economic nature'.[81] As long as economic activity can be separated, even if only in part, from the exercise of public powers, it is caught by competition law.[82]

According to the case law,[83] the situation might depend on the underlying legislation. If the authority directly operates the service and charges fees on a statutory basis, its activities, such as domain name registration, are unlikely to qualify as an economic activity and, thus, a service. It would fall outside of the DSA. On the other hand, if the state only maintains legal supervision of the domain name authority but the operations are entirely outsourced to a third party and fees charges at its discretion, they should qualify as an economic activity. Again, from my perspective, it is irrelevant whether such service is then run for-profit (eg Slovak SK-NIC) or as a non-profit activity (eg Czech CZ.NIC or EU's EURid).[84] Obviously, the inapplicability of the DSA's rules does not preclude the states from adopting their own liability exemptions, or due diligence obligations, to such activities. Due to the inapplicability of the DSA, such exemptions are not pre-empted either. Thus, if a Member State operates one or more of such digital services, it can simply extend or even modify due diligence obligations in its national legislation.

6.3 Emerging Difficult General Issues

Before turning attention to specific liability exemptions, I wish to further discuss some of the difficult points that I see on the horizon as potentially important for the effectiveness of the DSA.

[79] Case C-138/11 *Compass-Datenbank GmbH v Republik Österreich* ECLI:EU:C:2012:449, para 35.
[80] ibid para 35.
[81] ibid para 36.
[82] ibid paras 37–38.
[83] ibid paras 42–48.
[84] European Parliament and Council Regulation (EU) 2019/517 of 19 March 2019 on the implementation and functioning of the.eu top-level domain name and amending and repealing Reg (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004, art 9(2) on fees.

6.3.1 Impact of liability-excluding norms on liability-establishing norms

Liability exemptions function as liability exclusion provisions. They prevent European and national law, or their interpretation, from holding providers of such services liable. In other words, they only curtail the imposition of liability. The concept of 'liability for third party information' has an autonomous meaning, and it covers numerous areas of law, including civil, administrative, and criminal law, as long as the ultimate aim is to regulate the behaviour of content creators and hosts of such third-party information.[85] Similarly to the ECD, when the liability exemptions are no longer applicable because conditions are not fulfilled, it is up to other laws to establish any liability.[86]

The Directive's (the ECD), and now Regulation's (the DSA), rules merely harmonise the exemption of liability, not the liability itself—it does not provide a positive basis for establishing when a provider can be held liable, which will depend on other legal instruments at the European or national level. Thus, in theory, there can be a gap.[87] On the other hand, this also means that the unavailability of the exemption does not automatically lead to liability; such a provider can, from the European perspective, also be declared 'not liable'.

However, the relationship between liability exemptions and liability-establishing norms is further complicated by several factors.

First, the CJEU and national courts ocasssionally tend to establish liability at exactly the point where the exemption conditions are no longer satisfied (eg after a notice is not properly acted upon). Thus, the CJEU in *YouTube and Cyando* suggests that copyright liability for communication to the public will often coincide with a failure to satisfy the hosting liability exemption.[88] The judges applying liability-establishing rules alongside liability exemptions tend to be exposed to the anchoring effect of the exemptions. The two sets of rules thus can converge, although there is no legal requirement they do, and convergence can sometimes be counterproductive. This anchoring effect is not specific to EU law . Seeing liability exemptions as liability switches can be problematic because the policy reasons behind exempting liability can differ from those behind imposing it. The temptation to see what is exempted as the *only* appropriate course of conduct for a provider should be resisted. While for many services, such synchronisation of

[85] This issue was crucial in the pending Czech preliminary reference on unfair competition which was ultimately settled. Case C-470/22*: Request for a preliminary ruling from the Vrchní soud v Praze (Czech Republic) lodged on 14 July 2022—Česká národní skupina Mezinárodní federace hudebního průmyslu v I&Q GROUP, spol s r.o, Hellspy SE* [2022] OJ C418/12.

[86] The DSA does not impose the order in which the Member States apply the liability exemptions. They can, in theory, first apply liability provisions and then apply liability exemptions. However, this might sometimes risk misapplying the exemptions or applying them under the influence of national provisions. It might be more economical first to apply the liability exemptions and then liability provisions in national law, as the latter might have been devised long before these exemptions existed; thus, those liability provisions were not designed to avoid conflict.

[87] A good example is offered by the UK's Defamation Act 2013 in s 5. See also *McFadden* (n 22). However, the DSA offers a number of accountability obligations imposed on providers while they act within the liability exemptions.

[88] *YouTube and Cyando* (n 28) paras 79–84.

exemptions and liability norms might not create problems, for some types of services,[89] or some types of liability,[90] it could have draconian effects. Thus, the fact that establishing liability is still a job of another set of legal norms should be always remembered. Switching off the immunity shield does not automatically mean switching on liability for others.

Second, liability-establishing norms that have their basis in EU law can sometimes complement or modify the DSA safe harbours. Only very rarely, as with Article 17 of the Copyright in the Digital Single Market (CDSM) Directive,[91] do other EU rules specifically modify a liability exemption itself. Article 17 of the CDSM Directive introduces a special treatment for a subset of providers who are thereby explicitly excluded from the hosting exemption.[92] A different example is the General Data Protection Regulation (GDPR), which has a less explicit relationship with liability exemptions. For instance, the GDPR's understanding of some hosting services differs substantially from the logic underlying the liability exemption regimes. However, the conflict between these special rules and the liability exemptions is not always real because two areas of law often regulate related aspects of the same business (eg data protection law regulates data collection designed around the collection and distribution of users' content). In fact, the complementary relationship between liability exemptions and other EU instruments is a much more frequent occurrence (see Chapter 17). The EU acts, such as the Terrorist Content Regulation or Audiovisual Media Services Directive, are excellent examples. These rules are perfectly compatible with the liability exemptions and other rules of the DSA but might contain further specifications of what is expected in certain sectors.

6.3.2 Neutrality and reliance on factual presumptions

One of the interesting and unresolved problems related to liability exemptions is to what extent the exemptions limit the use of factual presumptions or other evidentiary heuristics by national courts.

In *Bastei Lübbe*,[93] the CJEU addressed the question of whether an owner of an internet connection can be 'presumed' to be the wrongdoer in some circumstances.[94] German courts have developed a doctrine according to which if the connection were prima facie solely used by its owner, he would be subject to a rebuttable presumption

[89] An example of this is applying the same standard to cloud computing providers involved in hosting on the infrastructure level.

[90] An example of this is applying the same standard to criminal liability for terrorist crimes or civil liability for defamation.

[91] CDSM Directive, art 17.

[92] CDSM Directive, art 17(3) ('the limitation of liability established in Article 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Article') and the DSA, art 89(2) ('References to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 4, 5, 6 and 8 of this Regulation, respectively'), and specifically also supported by the DSA, art 2(4)(b).

[93] Case C-149/17 *Bastei Lübbe GmbH & Co KG v Michael Strotzer* ECLI:EU:C:2018:841.

[94] ibid para 20 (summarising the case law). See also German Federal Supreme Court case, BGH v 27 July 2017 – Case I ZR 68/16.

that he acted illegally. This requires the owner to explain and provide evidence of the opposite; otherwise, he is liable for transmitted information.

While the owner could be said to have acted as a mere conduit if other parties were involved, such as his family members, the presumption forces him to substantiate that he is a mere conduit, eg by naming persons who could have used his service. The CJEU did not consider the liability exemption dimension of the dispute. It ruled that such rebuttable presumption is not only acceptable but arguably partly required for the effective enforcement of intellectual property rights.[95] This poses an important question for the mere conduit liability exemption, as well as other liability exemptions. Are such presumptions a form of 'liability for information transmitted'? If they are not rebutted, then this clearly manifests a liability for mere conduit service providers who may arguably be neutral (eg unaware co-tenants).

The difficulty with this rule is that the situation is akin to a national law that would condition the mere conduit exemption on disclosing some information. This would be incompatible with the DSA. However, if the rule is interpreted as a probability-based assessment of whether the mere conduit provider remained neutral, it could be more easily reconciled with Article 4 DSA. After all, the national courts must always make decisions in the context of factual uncertainty while relying on various heuristics.

This poses the question of *how far* the Member States and their courts can presume certain facts when the available evidence is limited. Undoubtedly, this question will come up before the CJEU. In *YouTube and Cyando*, the CJEU itself might be outlining an evidentiary standard concerning some of the infringements in copyright law that involves reliance on rebuttable presumptions.[96] Such presumptions were previously explicitly used by CJEU,[97] and thus, it is expected that the question of the limits of these presumptions will be tested sooner or later.

In its *YouTube and Cyando* judgment, the CJEU says that the following situations would fall outside the liability exemption and equally qualify as copyright infringement by the platform itself:[98]

- the provider 'participates in selecting' infringing content;
- the provider 'provides tools on its platform specifically intended for the illegal sharing of such content or that it knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform';
- the provider, 'despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological

[95] ibid paras 52–54.
[96] *YouTube and Cyando* (n 28) para 84.
[97] Case C-160/15 *GS Media BV v Sanoma Media Netherlands BV and others* ECLI:EU:C:2016:644.
[98] *YouTube and Cyando* (n 28) para 84; The case of Poland reiterates it as well, see *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297, para 27.

> measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform'.

The first two scenarios are easily understood as situations where the intention is present. To participate, one must possess a will to join the action deliberately. To *induce* by providing tools, one has to envisage their use for such a purpose. The CJEU cross-referred to its case law on *The Pirate Bay*,[99] a provider whose intentions were evident to anyone. When it comes to hosting, such users would be likely understood to act under the authority or control of the service provider.[100]

The last scenario is the most interesting. It seems to present an instance where the Court would be willing to *infer* the deliberate intent to participate in someone's wrong in the absence of other evidence of an initial common plan. In other words, it seems to envisage a scenario where deliberate collusion emerges from the interactions and mutual convenience of outcomes. In such a case, the Court appears to require evidence that the provider, once realising this, tries to counter this situation credibly and effectively. This does not mean it must do everything possible, but it must do more than pay lip service so that the Court may be convinced that it is not acting implicitly in concert. The Court's description of such a scenario suggests its *evidentiary nature*: when evidence of large-scale infringement is known to the provider, it must credibly dispel the suspicion that it is not acting in concert.

Basically, the burden of proof showing neutrality and lack of participation is shifted, following the establishment of some circumstances, to the provider who must dispel doubts about his neutrality and deliberate participation in the wrongs of others.

With this conceptualisation in mind, the standard is about a provider being a rogue player rather than failing once or twice. As a result, the evidence should be systemic, and the countermeasures neglected should be the low-hanging fruit that every reasonable actor would adopt in such a situation rather than the highest state of the art. After all, the test is used to *infer deliberate participation* in someone else's wrong—usually a high threshold. The intuition is that even if basic reasonable measures were withheld, and not applied, then the intentions of the hosting provider were not all that innocent and could have been aligned with those lawless users. In such a case, users do not misuse the service but use it as generally intended by the platform itself.

The CJEU will have to navigate the question of these presumptions delicately to maintain the balance the legislature tried to create. While, as in *McFadden*, it is understandable that the Court does not want to squeeze the procedural autonomy of the Member States, the lack of a common approach risks undermining the framework. The Court's passage from *McFadden* acts as a useful reminder of the conundrum:

[99] *The Pirate Bay* (CJEU) (n 54).
[100] DSA, art 6(2).

> It is not for the Court to take the place of the EU legislature by subjecting the application of that provision to conditions which the legislature has not laid down … To subject the exemption laid down in Article 12(1) of Directive 2000/31 to compliance with conditions that the EU legislature has not expressly envisaged could call that balance into question.[101]

6.3.3 The place of the neutrality test

Under the ECD, it was of no consequence whether the requirement of neutrality was understood as a test for 'provided information' or as a self-standing test derived from the recitals. Under the DSA, however, this changes. If the 'provided information' is stored by a provider, the DSA's due diligence obligations apply even if the provider is not neutral. In contrast, if the information is interpreted as not 'provided by recipients', even though a provider stores it, the DSA's due diligence obligations do *not* apply.

Recital 29 stresses that:

> Whether a specific service constitutes a 'mere conduit', 'caching' or 'hosting' service depends solely on its technical functionalities, which might evolve in time, and should be assessed on a case-by-case basis.

Thus, the Recital makes clear that no other criteria, including neutrality, should be applied to the question of whether a service is regulated by the DSA. A contrario, this is also confirmed by Recital 18, which only says that '[t]he *exemptions from liability* established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information'. Thus, the rest of the Regulations can continue to apply to them. This reading is reinforced by Recital 41 stating that '[t]he due diligence obligations are independent from the question of liability of providers of intermediary services which need therefore to be assessed separately.'

Finally, a similar point can be derived from Article 7. While the ECD included a cross-reference to a provider 'when providing the services covered by Articles 12, 13 and 14', the DSA refers merely to 'intermediary services' and the technical activities of transmitting or storing. This could be read as a mere simplification of the text. However, considering the above discussion, it stipulates that the prohibition of general monitoring *does* apply *whenever* providers exercise those technical functions, *regardless* of whether they eventually lose a liability exemption because they stop being neutral (see Chapter 5).

[101] *McFadden* (n 22), paras 69–70.

Table 6.2 Legal concepts and their consequences

Legal concept	Legal consequences
Service as an 'economic activity'	» determines whether the DSA applies at all.
Activity as 'hosting', 'mere conduit', 'caching'	» determines whether the DSA applies at all.
Information is 'provided by' recipients of the services at their 'request'	» determines whether the DSA applies at all;
The 'neutrality' of the provider vis-à-vis provided information	» determines whether the liability exemptions apply but not whether the due diligence obligations still apply; thus, services that adopt or instruct users' content do not benefit from exemptions but might become VLOPs.

In my view, the DSA tries to make it clear that apart from the neutral intermediaries who benefit from Article 8, the provision also applies *whenever* due diligence obligations are imposed, including on non-neutral intermediaries.[102] This is because the DSA, per Recital 30, explicitly submits its entire Regulation, and thus also the due diligence framework, to Article 8 scrutiny.[103] Thus, for instance, a provider of generative artificial intelligence (AI) that draws from submitted user-generated content is likely to be non-neutral vis-à-vis its input is unlikely to be covered by liability exemptions. However, such a provider remains subject to the DSA due diligence obligations and the Prohibition on General Monitoring (GMOP) and can become a very large online platform (VLOP).

This is not to say that Court should not delimit the scope of the DSA by interpreting the notion of 'provided information'. Such test remains crucial to distinguish between user-generated-content services, and those without such a component. The courts and authorities have all the incentives to frame the test for 'provided information' very broadly if they wish to keep the scope of the applicability of due diligence obligations broader than the concept of neutrality. As far as liability exemptions are concerned, any over-broadness can still be mitigated through an independent narrower test of the neutrality of services. To illustrate this, consider the difference between two types generative AI systems: a) services built on top of content of users submitted them, and b) services built by pulling the content from the web. The former, as mentioned above, can qualify as hosts, but can still sometimes lack neutrality vis-à-vis their outputs. However, the latter cannot qualify as hosts because they are not provided with such user-generated content at all. The outcome then appears as shown in Table 6.2.

[102] This is not that unconventional. The CJEU already held that the GMOP can still apply, eg in areas not covered by liability exemption, even in the offline context. For more on the debate, Husovec (n 27) 118.

[103] DSA, Rec 30 states that '[*n*]*othing in this Regulation* should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content' (emphasis added).