7

Liability Exemptions: Specific Services

7.1 Introduction

The three Digital Services Act (DSA) liability exemptions discussed in the previous chapter are built around different expectations. First, conduit immunity mostly expects providers to cooperate with the state authorities by following their orders. Second, the caching immunity expects speedy catch-up with those whose infringements they mirror. And finally, the hosting immunity imposes choreography of non-judicial notice and takedown upon providers. Each liability exemption has its own rules and specifics, which I will try to explain in this chapter. Some composite services, such as messaging apps or search engines, can see their different components fall under more than one liability exemption depending on how they operate (Chapters 7.6 and 9.2).

7.2 Mere Conduits

Article 3(g)(i) DSA defines the mere conduit services as 'consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network'. Article 4 DSA then details the liability exemption as follows:

> Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the service provider shall not be liable for the information transmitted or accessed, on condition that the provider: …

The logic behind the legal intervention remains the same as in 2000. The lowest parts of the technical infrastructure 'stack' are not expected to control the content that flows

through the 'pipelines' (Chapter 1). As much as postal services are not liable for the content of the letters and packages exchanged, internet infrastructure needs to have the same legal certainty that by facilitating, transmitting, and giving access to content which might be illegal, they are not, nor do they want to be, assuming any legal risk. The mere conduit exemption does this important job.

The provision covers services that provide 'transmission' or 'access to' any communication network. Unlike Article 12 E-Commerce Directive (ECD), the DSA's text now explicitly covers liability for 'transmission' *and* giving 'access to' such provided information. The new wording extends the functionality of the provision. For instance, a pub owner who electronically and at a distance only provides codes to an open wi-fi operated by another company previously could not claim the liability exemption for the misuse of connectivity. Although such a pub owner gave access to a network, since liability was only exempted as regards the 'transmission', which he never carried out, there was no protection. Now, a pub owner can equally invoke the mere conduit provision because it is not liable for giving 'access'.

The new wording was a long overdue demand by technical intermediaries who felt that the original liability exemption was too narrowly worded to cover only typical internet access providers. For years, various online intermediaries, such as content delivery networks or domain name registrars and registries, were unsure of whether they could invoke any exemptions. While many courts in the Member States often gave them some liability assurances,[1] the status quo did not help the internal market and caused fragmentation.

Recital 29 of the DSA now provides a long list of examples that intend to extend the application of the exemption to 'generic categories of services, such as internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-level domain name registries, registrars, certificate authorities that issue digital certificates, voice over Internet Protool (IP) and other interpersonal communication services'.[2] It suggests the interpretation that providers of domain name services, such as domain name authorities (eg EURid), or domain name resolvers, are covered as mere conduits.[3] These services can be said to provide *access* to the communication network, the internet, by offering a particular type of access service, being a translation

[1] In the German case of *ambiente.de,* the German Federal Supreme Court rejected the imposition of obligations on a domain name authority, citing the public interest in the cheap DNS infrastructure (BGH v 17 May 2001—I ZR 251/99). The Slovak Supreme Court reached a similar outcome on 12 July 2007, 3 Obo 197/06, *rover.sk*. See also the US case of *Lockheed Martin Corp v Network Solutions Inc* 141 F Supp 2d 648 (ND Tex 2001).

[2] Description of technical functioning, examples of services covered by art 12 ECD as well as 'grey areas' are provided by Sebastian Schwemer, Tobias Mahler, and Håkon Styri, *Legal Analysis of the Intermediary Service Providers of Non-Hosting Nature: Final Report* (EU Publications Office 2020).

[3] The only relevant case to date was Case C-521/17 *Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta* ECLI:EU:C:2018:639. However, the case did not clarify the issue. In the literature, Schwemer and colleagues expressed some doubts, but they did not seem to consider access-only mere conduits (probably influenced by the ECD's original language). Their argument about domain name authorities providing 'pointers' is very much in line with the argument that such services provide access to the network, see Sebastian Felix Schwemer, Tobias Mahler, and Håkon Styri, 'Liability Exemptions of Non-Hosting Intermediaries: Sideshow in the Digital Services Act?' (2021) 8(1) Oslo Law Review 4, 14.

of an IP address to a domain name.[4] The same applies to other services not mentioned in Recital 29, such as browsers, operators of nodes that help to re-route the internet traffic (eg Tor), and providers of video-communication tools (eg Zoom) or potentially even some operating systems.

This new wording should thus encourage national courts to apply the provision to less traditional infrastructure services[5] and keep an open mind to new technological developments. Recital 29 acts as a sort of non-exhaustive, open list, referring to 'a wide range of economic activities which take place online and that develop continually to provide for transmission of information that is swift, safe and secure, and to ensure convenience of all participants of the online ecosystem'.

A typical example of a service introduced to consumers only in the early 2000s is wi-fi hotspots. Today, wi-fi hotspots are ubiquitous—every hotel, public space, and restaurant offers a connection. Individuals share their internet connection with visitors. Wi-fi connection is promoted by states, including the European Union (EU).[6] Only in 2016, however, did the Court of Justice of the European Union (CJEU) clarify that the providers of wi-fi hotspots benefit from the mere conduit liability exemption.[7]

For Article 4 DSA to apply, the relevant network does *not* have to be *public*. This means that transmission or access can relate to closed or private networks. Thus, even providers of some messaging apps can also be seen as providing transmission within and access to a communication network—the infrastructure allowing the connection between different phones. They also transmit the information. However, the problem that these messaging apps face is the issue of the duration of storage. According to Article 4(2) DSA:

> The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

The word 'transmission' suggests that the storage of information must only be transient. Although Article 4(2) DSA specifies that this 'includes' some forms of transient

[4] DNS resolvers offer a technical translation service between a numerical IP address and an alphabet-based domain name (eg 2001:4860:4860::8888 for Google.com). Since such a translation service does not transmit the data (website's content), it only provides simplified access to the communication network. The question remains how the CJEU will apply art 4(2) DSA, ie whether the IP address in the registry is seen as a tool of access or rather information to be stored only temporarily to enable transmission by someone else.

[5] See, for instance, the Hamburg Regional Court ruling regarding DNS providers such as Quad9, LG Hamburg v 12 May 2021—310 O 99/21.

[6] European Parliament and Council Regulation (EU) 2017/1953 amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of internet connectivity in local communities [2017] OJ L286/1. The Commission proposal mentioned the intermediary liability question related to the provision of wi-fi hotspots (Wifi4EU), see Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of Internet connectivity in local communities' COM(2016) 589 final.

[7] Case C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:689.

storage, the word 'transmission' would still limit the storage. Messaging apps can operate in different ways. They can involve 'permanent' or only transient storage. The former would seem to exclude the application of the mere conduit exemption. In such cases, messaging apps relying on cloud-based storage might qualify as hosting providers instead (see section 7.6). On the other hand, if messaging apps only allow users to store the messages locally and only transmit the information, they can continue to qualify as mere conduits because they provide 'access' to the communication network.[8] The likely test for 'transmission' is whether the period of storage is 'longer than is reasonably necessary for the transmission', according to Article 4(2) DSA.

Apart from the overarching neutrality requirement (Chapter 6.2.4), the conditions for mere conduit liability exemption are that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. Once these conditions are fulfilled, Article 4 DSA confers near-absolute immunity that cannot be retracted even by obtaining knowledge. Thus, an access provider notified about the illegal activity of a website on the internet has no general legal obligation to step in and block it for its customers. While authorities might be able to require the blocking, such orders or legislation must target specific websites (Chapters 5 and 8).

These three conditions are meant to prevent rogue actors from misusing the exemption to shield their illegal operations from liability. For instance, if a hotel owner providing open wi-fi were to instruct her employees or clients to engage in some illegal actions, the exemption would not apply. She could be said to have initiated the transmission or influenced what was transmitted. In such a case, the service provider 'deliberately collaborates with a recipient of the services in order to undertake illegal activities'.[9] The DSA and the ECD conceptualised such situations as active interventions that disqualify the mere conduit from the passive provision of the service. The same logic underlies the explicit requirements in Article 4(1) DSA against the initiation of *who* receives *what* transmission from *whom* on the network. The provider selecting any of these components is no longer a mere conduit.

If all the conditions are met, mere conduits cannot be held liable for the third-party information they have transmitted or given access to. Once the mere conduit liability exemption is inapplicable, the national law is free to impose liability.

7.3 Caching

Article 3(g)(ii) defines the caching services as 'consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for

[8] But not as online platforms, as those exclude pre-approval (see DSA, Rec 14).
[9] ECD, Rec 44; DSA, Rec 20.

the sole purpose of making more efficient the information's onward transmission to other recipients upon their request'. According to Article 5 DSA, its regime is defined as follows:

> Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, the service provider shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient or secure the information's onward transmission to other recipients of the service upon their request, on condition that the provider: …

Again, this provision is based on Article 13 ECD, which is the least litigated liability exemption of the three. The only change in the wording brought about by the DSA is the addition of the words 'or secure' when discussing the purpose of transmission. This alteration was motivated by the desire to capture the changing face of content delivery networks that increasingly not only, or not primarily, facilitate better and faster access to the network by providing geographically closer servers with copies of websites but also help to resolve and protect from various cybersecurity incidents, such as Distributed Denial-of-Service (DDOS) attacks. This regulatory change was already identified by the Commission in its Impact Assessment.[10]

Apart from the neutrality requirements, the specific operational requirements include: a) not modifying the underlying information, b) complying with the conditions on access to it, c) the industry rules regarding the temporal aspects of caching, and d) not interfering with the lawful use of technology to obtain data on the use of the information.[11] Finally, it is expected that the:[12]

> Provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

The caching exemption thus presents an immunity model close to hosting but with some additional protections. Caching services are not required to act upon notification if the targeted content was not removed from the original servers. They are generally only asked to *assess* whether the notified content was removed or disabled on the source website. If it was, an expectation to remove it is triggered; or the provider might expose

[10] 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 (Digital Services Act) and Amending Directive 2000/31/EC"' SWD(2020) 348 final, annex 9. This change was also favoured by Schwemer and colleagues, see Schwemer, Mahler, and Styri (n 2) 36.

[11] DSA, arts 5(1)(a)–(e).

[12] DSA, art 5(1)(e).

itself to liability. However, as long as it is still on the source website, actual knowledge of the illegality of information does not create any expectation to act. The only exception is if there is an order from an authority demanding the removal of such information. That order can also target the source website, which only refuses to implement it. An order targeting the caching provider must also comply (Chapter 8). Although compliance with the latter order is not presented as one of the conditions in Article 5(1)(e), it should equally lead to the loss of an exemption (argument *a minore ad maius*).

Examples of caching include stand-alone caching services and, increasingly, Content Delivery Networks (CDN), which incorporate caching services. The CDNs can be seen to incorporate various types of technical activities. Some of them can qualify as caching (temporary mirroring of content to a geographically closer location), hosting (for longer web hosting) or even mere conduit (a proxy reverse function that acts as an access point).[13] This variety has also been identified and discussed in increasingly rich case law, particularly in Italy and Germany, where courts have struggled to determine whether the CDN services belong to a particular liability exemption and, if so, to which one.[14] It remains to be seen whether the wording change and the clarification in Recital 29 mentioning the CDNs, together with reverse proxies or content adaptation proxies, will be sufficient to provide greater legal certainty.

In European case law, two other types of services are sometimes discussed in connection to caching. The first type of service is search engines that index the internet and create a 'cache' memory of its content to offer search results. Their potential status as caching services was fiercely debated in the negotiations of the DSA, as explained below. The second service is live streaming services, which is not mentioned in the DSA despite its increasing popularity. Livestreaming is often provided by dedicated services (such as Periscope), social media (such as Facebook), and video-sharing platforms (such as YouTube). Given the immediacy of the provision of content, these services fall in between traditional broadcasting, on-demand audio-visual services and digital user-generated services. The Commission detailed the potential qualification of livestreaming services in its Impact Assessment.[15] However, those considerations led to little changes in the DSA's text. This silence, however, should not, in my view, be interpreted as an exclusion but rather as calling for a 'case by case' assessment of the service at hand.

7.4 Hosting

Unlike the mere conduit services, which mainly cover the modern infrastructure behind the communication networks, hosting services often apply to the application

[13] For the description and debate under the ECD framework, Schwemer, Mahler, and Styri (n 3).

[14] See the Rome Commercial Court case, *Mediaset (RTI) vs Cloudflare* (2019) Case No 1932/2019 which was subsequently confirmed in Rome Commercial Court, *Mediaset (RTI) v Cloudflare* (2019) Case No 26942/2019; Cologne District Court case, LG Köln v 05.12.2019—Case 14 O 171/19 (*Universal Music GmbH v Cloudflare*).

[15] Commission, 'SWD(2020) 348 final' (n 10) annex 9.

layer of the internet's technology stack. They cover services ranging from social media, discussion fora, online marketplaces, review websites, video-sharing services, and more. At the same time, the same exemption also applies to some infrastructure services, such as web-hosting services. Recital 29 DSA includes, eg 'categories of services such as cloud computing, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing'.

Admittedly, the presence of infrastructure-like services among mostly application-layer services is exceptional and requires careful distinguishing. As noted below, the DSA creates a new category of hosting services—online platforms—that better describes the application layer because they store and distribute information to the public as one of its main goals. All other hosting services that are not only excluded from the term due to their small size usually cover 'mere hosting' services that tend to cover the infrastructure, such as web hosting.

Article 6 DSA provides that:

> Where an information society service is provided that consists of the storage of information provided by a recipient of the service the service provider shall not be liable for the information stored at the request of a recipient of the service on condition that the provider: …

This wording mirrors that of Article 14 ECD, hence validating the legal approach supported by the ECD for 20 years and interpreted extensively by the CJEU. The scope of services remained unchanged. The CJEU so far has accepted the following services as covered by the hosting safe harbour: social media,[16] online marketplaces,[17] video-sharing platforms,[18] cyber-lockers,[19] and keyword-based advertising on search engines.[20] Other services that consist of 'storage of information' provided by others include storage of comments on blogs,[21] or on social media by page administrators,[22] services of app stores, cloud services and web hosting, distribution of Really Simple Syndication (RSS) feeds,[23] storage of user reviews,[24] and user offers of accommodation on sharing economy platforms.

The hosting safe harbour is subject to two main conditions. They apply if the provider:

[16] Case C-360/10 *SABAM v Netlog NV* ECLI:EU:C:2012:85; Case C-70/10 *Scarlet Extended SA v SABAM* ECLI:EU:C:2011:771; Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821.

[17] Case C-324/09 *L'Oréal SA and others v eBay International AG and others* ECLI:EU:C:2011:474.

[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:2021:503 (*YouTube* and *Cyando*); Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297.

[19] *YouTube and Cyando* (n 18).

[20] Joined Cases C-236/08 to C-238/08 *Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2010:159.

[21] See, for instance, German Federal Supreme Court, BGH v 25 October 2011—Case No VI ZR 93/10; *Payam Tamiz v Google Inc* [2013] EWCA Civ 68.

[22] The administrators of pages are hosting providers along with social networks.

[23] German Federal Supreme Court, BGH v 27 March 2012—VI ZR 144/11.

[24] German Federal Supreme Court, BGH v 23 June 2009—VI ZR 196/08 (Spichmich.de).

> (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; and (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.[25]

This wording again mirrors Article 14 ECD. Thus, all the pre-existing case law of the CJEU can apply to these requirements without any changes. According to CJEU in *Poland*, 'for such an operator to be excluded, under Article 14(1)(a) of that directive, from the exemption from liability provided for in Article 14(1), it must have knowledge of or awareness of specific illegal acts committed by its users relating to protected content that was uploaded to its platform'.

The Court thus confirmed its earlier Grand Chamber ruling in *L'Oreal v eBay*, which held that knowledge under (b) can be obtained only by sufficiently precise and adequately substantiated notice.[26] In *YouTube and Cyando* and *Poland*, the Court also confirms that awareness itself must concern specific illegal acts. Typically, one can imagine that headline news about a case in the mainstream media can lead to awareness. The DSA, however, reiterates the original language of Article 14 of the ECD, which limited this standard of knowledge to only liability for damages. This means that on the national level, in situations where 'awareness' exists but 'actual knowledge' is absent, liability can be imposed only in the form of damages.[27] This has important consequences for various forms of criminal liability, which would always need to clear the hurdle of actual knowledge. In most cases, awareness and actual knowledge coincide as types of knowledge, but only the former can be derived from a broader set of circumstances.

In contrast, mere general awareness (abstract knowledge) of illegal activity is in itself insufficient. The DSA now dispels some of the doubts previously left open by the ECD. First, Recital 22 clearly says that relevant 'actual knowledge or awareness cannot be considered to be obtained solely on the ground that that provider is aware, in a general sense, of the fact that its service is also used to store illegal content'. Second, for the first time, the law specifies the common Union requirements for notification in Article 16 DSA, which are based on previous case law. These requirements act as statutory clarifications of what type of notifications can lead to the hosting providers opening up to liability. The book extensively describes these requirements in Chapter 11.

In short, according to the *eBay* decision, the CJEU does not limit the acquisition of knowledge to notification only. In *eBay*, the Court held that:

> Moreover, if the rules set out in Article 14(1)(a) of Directive 2000/31 are not to be rendered redundant, they must be interpreted as covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances. The situations thus covered include, in particular, that in which the operator

[25] DSA, arts 6(1)(a)–(b).
[26] *eBay* (n 17).
[27] Miquel Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (2009) 32 Columbia Journal of Law & the Arts 481.

> of an online marketplace uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information. In the second case, although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, given that notifications of allegedly illegal activities or information may turn out to be *insufficiently precise or inadequately substantiated*, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality.[28]

The standard of 'sufficiently precise' and 'adequately substantiated' notifications is now cemented in the DSA through various provisions—Recitals 22 and 53 and Articles 16(2) and 20(3). The key summary is provided by Recital 53, which also incorporates *YouTube and Cyando*'s[29] recent clarification of the underlying standard of assessment of facts:

> Where a notice contains sufficient information to enable a diligent provider of hosting services to identify, without a detailed legal examination, that it is clear that the content is illegal, the notice should be considered to give rise to actual knowledge or awareness of illegality.

A diligent economic operator serves as a benchmark for care with which providers must assess any sources of information. This is also the reading given to the provision by the national courts.[30] The CJEU is slowly developing the standard across various legal instruments. For instance, in data protection law, the delisting requests concerning factual inaccuracies in search engines must meet the threshold of the 'manifest' or 'obvious inaccuracy' that must be corroborated by evidence that 'can reasonably be required' in the circumstances.[31] In *TU and RE v Google*, the Court explained the underlying rationale most vividly:

> … when assessing the conditions for application laid down in Article 17(3)(a) of the GDPR, that operator cannot be required to *play an active role in trying to find facts* which are not substantiated by the request for de-referencing, for the purposes of determining whether that request is well founded … the operator of the search engine

[28] *eBay* (n 17) paras 121–22 (emphasis mine).
[29] *YouTube and Cyando* (n 18).
[30] In *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2016] NICA 54 [69]–[72], the Northern Irish Court of Appeal found that omission of the correct form of legal characterisation of the claim ought not to be determinative of the knowledge of facts and circumstances; rather, the perspective should be one of the diligent economic operators.
[31] Case C-460/20 *TU and RE v Google LLC* ECLI:EU:C:2022:962, paras 68 and 72 (using the word 'obvious').

> concerned *cannot be required to investigate the facts and, to that end, to organise an adversarial debate with the content provider* seeking to obtain missing information concerning the accuracy of the referenced content … such an obligation would impose on that operator *a burden in excess of what can reasonably be expected of it in the light of its responsibilities, powers and capabilities* … would thereby entail a serious risk that content meeting the public's legitimate and compelling need for information would be de-referenced and would thereby become difficult to find on the internet. In that regard, there would be *a real risk of a deterrent effect on the exercise of freedom of expression and of information if the operator of the search engine undertook such a de-referencing exercise quasi-systematically*, in order to avoid having to bear the burden of investigating the relevant facts for the purpose of establishing whether or not the referenced content was accurate.[32]

The Court's reasoning thus makes clear that the knowledge standard prevents the providers from being subject to a post-notification obligation 'to play an active role in trying to find facts'. As was argued in Chapter 5, this is entirely in line with the overarching principle of a shared burden for social harms.

The DSA, however, puts more pressure on the notification process through due diligence obligations. Post-DSA, it will be much harder for hosting providers to disregard notifications. The DSA specifies *who* and in *what form* shall receive them. However, the broad scale of possibilities might be limited by the availability of evidence in practice. If a hosting provider acts on its own initiative (Article 7 DSA) and uncovers unlawful content that it disregards, the outside world might not have sufficient evidence to prove that this omission happened unless they get access to non-public information held by such providers. Therefore, notifications remain the most important and documentable vehicle for imparting knowledge about certain illegal acts.

In *YouTube and Cyando*, the Court clarifies that in determining whether the provider intervened, the relevant factors to consider include even circumstances where the provider who '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 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'.[33] As explained in Chapter 6, I see this requirement as pertaining to the neutrality of the hosting provider, and not as a separate knowledge standard. It speaks to the issue of whether the hosting provider collaborates with its infringers. The CJEU's re-statement of the *YouTube and Cyando* ruling in *Poland* seems to confirm this.[34] As a result, general awareness is never sufficient to trigger knowledge. However, a failure to keep up with the threats on one's

[32] ibid paras 70–71 (emphasis mine).
[33] *YouTube and Cyando* (n 18) para 84.
[34] *Poland* (n 18) para 28; *YouTube and Cyando* (n 18) paras 117–18.

own platform, to the extent that the provider is unwilling to counteract them by any credible means, can allow the courts to *infer* that platforms deliberately and intentionally collaborate with their lawless users. The evidence bolstering such inference should be serious (Chapter 6.2.4).

Since a good part of the DSA concerns hosting providers, a great deal of attention will be dedicated to them in the following chapters. Hosting exemption is, without a doubt, the heart of the DSA Regulation. Its preservation was never questioned by the Commission in its proposal or by co-legislators during negotiations.[35] The category of online platforms, including very large online platforms, is only its subset of hosting services. The DSA disentangles the due diligence obligations that apply to all hosting service providers by dividing them into several categories: 'just' hosting (eg cloud and web hosting) and online platforms, including very large online platforms (VLOPs). This is clearly explained in Recital 13, where co-legislators reinforced the need to exclude infrastructure services from the category of platforms:

> … For the purposes of this Regulation, cloud computing or web-hosting services should not be considered to be an online platform where dissemination of specific information to the public constitutes a minor and ancillary feature or a minor functionality of such services. Moreover, cloud computing services and web-hosting services, when serving as infrastructure, such as the underlying infrastructural storage and computing services of an internet-based application, website or online platform, should not in themselves be considered as disseminating to the public information stored or processed at the request of a recipient of the application, website or online platform which they host.

However, the DSA drafting also shows that some types of services are under separate regulatory scrutiny, even among online platforms. The most vivid example is online marketplaces, which I will discuss next.

7.4.1 Specifics of online marketplaces as hosts

During the legislative debate, the biggest pressure to deviate from horizontal rules concerned online marketplaces and their situation in consumer law.[36] In Chapter 6.2.4, I explained why providers that fail to disclose the source of content could lose their neutrality. This was a key concern for the consumer interest groups. Online platforms that act as marketplaces and sellers in those marketplaces can cause a risk of confusion for average consumers.[37] In the legislative process, the

[35] Folkert Wilman, 'The EU's System of Knowledge-Based Liability for Hosting Service Providers in Respect of Illegal User Content—Between the e-Commerce Directive and the Digital Services Act' (2021) 12(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 317, 318.

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

[37] While the Commission proposal referred to an 'average and reasonably well-informed consumer', the co-legislators, particularly the EP, limited the reference to an 'average consumer'. However, this should not have any

questions around the specific liability of online marketplaces for product safety were considered to be 'too sector-specific' and better suited for the concurrent discussions around the review of the General Product Safety Directive[38] and the Product Liability Directive.[39] These negotiations ran in parallel and were equally informed by the existing and upcoming CJEU case law.

Article 6(3) of the DSA eventually states the following:

> Paragraph 1 shall not apply with respect to the liability under consumer protection law of online platforms that allow consumers to conclude distance contracts with traders, where such an online platform presents the specific item of information or otherwise enables the specific transaction at issue in a way that would lead an average consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.

Based on the definition of online marketplaces under the consumer acquis,[40] the provision seems limited to 'B2C' relationships and thus excludes consumer-to-consumer exchanges. However, as explained in Chapter 6.2.4, in my view, this provision only represents a broader rule grounded in the condition of neutrality of providers. The standard is clearly inspired by pre-existing CJEU case law in EU consumer protection law[41] and the general neutrality requirement.[42] Moreover, as shown below, it was recently further validated by certain developments in EU trademark law.

Following an Opinion of AG Szpunar,[43] the CJEU recently held in *Louboutin v Amazon* that the operator of a marketplace could itself directly violate the trademark law when it sells products of others:

practical effects; as for the CJEU, the two are in a relationship of a concept and a benchmark in many areas, including consumer and trademark law; see Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L095/29, Rec 18; and Case C-470/93 V*erein gegen Unwesen in Handel und Gewerbe Köln eV v Mars GmbH* ECLI:EU:C:1995:224.

[38] European Parliament and Council Regulation (EU) 2023/988 on general product safety, amending Regulation (EU) No 1025/2012 and Directive (EU) 2020/1828, and repealing General Product Safety Directive 2001/95/EC and Directive 87/357/EEC [2023] OJ L 135/1 (General Product Safety Regulation).

[39] Commission, 'Proposal for a directive of the European Parliament and of the Council on liability for defective products' COM(2022) 495 final (still in the legislative process at the time of writing).

[40] Art 2(n) of Directive 2005/29/EC as amended by Directive (EU) 2019/2161: ' "online marketplace" means a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers'; European Parliament and Council Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22, as amended by Directive (EU) 2019/2161 (Unfair Commercial Practices Directive).

[41] Case C-149/15, *Sabrina Wathelet v Garage Bietheres & Fils SPRL* ECLI:EU:C:2016:840, para 41.

[42] *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2020:586, Opinion of *AG Øe*, para 152.

[43] Joined Cases C-148/21 and C-184/21 *Christian Louboutin v Amazon and others* ECLI:EU:C:2022:422, Opinion of AG Szpunar, paras 67, 71, and 73.

> … where, in view of all the circumstances of the situation in question, such a user may have the impression that that operator itself is marketing, in its own name and on its own account, the goods bearing that sign. In that regard, the following are relevant: the fact that that operator uses a uniform method of presenting the offers published on its website, displaying both the advertisements relating to the goods which it sells in its own name and on its own behalf and those relating to goods offered by third-party sellers on that marketplace; the fact that it places its own logo as a renowned distributor on all those advertisements; and the fact that it offers third-party sellers, in connection with the marketing of goods bearing the sign at issue, additional services consisting inter alia in the storing and shipping of those goods.[44]

The proposed reading of the neutrality test in Chapter 6 would produce the same outcomes as the *Louboutin* case and Article 6(3) DSA.

The Commission's proposal of the text of Article 6(3) was subject to strong discussions, in particular in the European Parliament (EP) Committee on the Internal Market and Consumer Protection (IMCO). The IMCO Committee favoured a much more radical approach. It proposed a new provision entitled 'liability of online platforms allowing consumers to conclude distance contracts with traders'.[45] The provision would (a) make the liability exemption conditional to the compliance with due diligence obligations or information requirements under consumer law;[46] (b) exclude the exemption of liability to online marketplaces for traders from third countries when there is no economic operator inside the EU, or the product is non-compliant; and (c) exclude the liability exemption where the online marketplace exercises 'decisive influence'. The concept of 'decisive influence' was proposed by some academics,[47] and consumer protection organisations have adopted it as their recommendations.[48] The concept was a combination of the neutrality test, further expanded by the criteria extracted by the CJEU in the *Uber* case to conclude that UberPop was not an information society service, but rather a transport service.[49]

[44] Joined Cases C-148/21 and C-184/21 *Christian Louboutin v Amazon and others* ECLI:EU:C:2022:1016, para 54.

[45] Committee on the Internal Market and Consumer Protection, 'Draft Report on the 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 (COM(2020) 0825) (2021) 66.

[46] Adding such a link would, for instance, mean that (a) online marketplaces can be held liable for any infringement to the due diligence obligations, for instance, not to appoint a legal representative, which could be seen as disproportionate; and (b) compliance with such due diligence obligations would happen to be almost voluntary, as it would merely be an incentive to be covered from liability.

[47] Christoph Busch, Gerhard Dannemann, Hans Schulte-Nölke, Aneta Wiewiorowska-Domagalska, and Fryderyk Zoll, 'The ELI Model Rules on Online Platforms' (2020) 9 Journal of European Consumer and Market Law 61.

[48] The European Consumer Organisation (BEUC), 'Making the Digital Services Act Work for Consumers—BEUC's Recommendations' (BEUC 2020) 6.

[49] Case C-434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain* ECLI:EU:C:2017:9811.

The proposal was rejected by the EP plenary, and it was not included in the EP's mandate. However, some elements were adopted in the recitals as potential guidance to interpret two important elements of the liability exemption for marketplaces. Recital 23 states that where the provider of an online platform allows consumers to conclude distance contracts with traders and it determines the price of the goods or services offered by the trader, it 'could' act under the control or authority of the provider of hosting services for Article 6(2) of the DSA. Article 6(3) of the DSA is further explained by Recital 24, which states some of the examples that 'could' be subsumed here, such as a failure to display clearly the identity of the trader pursuant to the DSA, withholding the identity or contact details of the trader until after the conclusion of the contract, or where an online platform markets the product or service in its own name rather than in the name of the trader who will supply that product or service.

The legislature's rejection of the concept of 'decisive influence' clearly rejected three specific criteria. Firstly, whether contracts were concluded in a 'closed environment', as it was felt that this could worsen the consumer experience and safety. Secondly, where the platform operator helps to prepare the terms of the trader-consumer contract, such as the form of consent, deadlines for withdrawal of consent, or delivery, feared to discourage uniformity and, once again, user safety. Finally, the idea of using the provision to discourage specific payment systems was also rejected because such systems are seen as great enhancers of trust rather than aggressive control techniques by providers. This was previously also recognised by the CJEU in *Airbnb*.[50]

In conclusion, Article 6(3) is merely a further statutory manifestation of the underlying neutrality test that underlines the entire framework (Chapter 6.2.4).

7.5 Search Engines

It seems that European regulation of digital services has been, for more than two decades, unable to decide how to explicitly deal with at least one set of services—search engines. These services help to organise information for users. Specialised price-comparison search engines help consumers to select service providers and producers of their liking. Search engines, like Google Search or Bing, build an index of information and market offerings from all around the world, helping users to navigate the Web by crawling the Web and creating an index, often without seeking permission. While these services already existed at the time of the ECD's drafting, they were not explicitly addressed in the liability exemptions. The DSA largely repeats this course of action.

[50] Case C-390/18 *Airbnb Ireland* ECLI:EU:C:2019:1112, paras 62, 64.

The US Digital Millennium Copyright Act (DMCA), the ECD's counterpart and direct inspiration, included search engines as a separate category of exempted services.[51] Recital 18 of the ECD mentions search engines only in a recital as an example of information society services. The legislative history seems unclear, but from the historical documents, it appears that the revision clause in Article 21 of the ECD could have been added as a response to the Irish insistence to create a separate rule for search engines.[52] In its first implementation report (2003) on the ECD, the Commission reported that:

> In addition to the matters dealt with by Articles 12–14, some Member States decided to provide for limitations on the liability of providers of hyperlinks and search engines. This was motivated by the wish to create incentives for investment and innovation and enhance the development of e-commerce by providing additional legal clarity for service providers. Whilst it was not considered necessary to cover hyperlinks and search engines in the Directive, the Commission has encouraged Member States to further develop legal security for internet intermediaries. It is encouraging that recent case-law in the Member States recognizes the importance of linking and search engines to the functioning of the internet.[53]

Hungary, Poland, Portugal, and Spain have opted to extend the hosting immunity to the activities of search engines, while Austria, following an intense legislative debate, switched to the conduit model.[54] However, the practical impact of such exemptions is often unclear. In Austria, Article 14 of the Austrian E-Commerce Law does not allow any 'selection' or 'modification' of the information, and the provision was inapplicable to liability in image search due to modification of the indexed content, which could be equally problematic for text search results.[55]

[51] 17 USC § 512.

[52] Permanent Representatives Committee, 'Extract of the Summary Record of the 1853rd Meeting of the Permanent Representatives Committee on 17 and 19 November 1999' (1999) Doc 12957/99 Ext 1 CRS/CRP 44 ECO 387 CONSOM 73 CODEC 714, 4 <https://resources.law.cam.ac.uk/cipil/travaux/ecommerce_directive/ecommerce_travaux_complete.pdf#page=325> accessed 5 August 2023 ('[Ireland] continued to propose an additional article on search engines'). However, Hoboken reports that proposals covering search engines were also tabled by the European Parliament, Joris van Hoboken, *Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines* (Kluwer Law International 2012) 230 (however, with an unclear reference to sources).

[53] Commission, 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)' COM(2003) 0702 final, para 67.

[54] ibid. See Austria: art 14 of E-Commerce-Gesetz (BGBl I Nr 152/2001) (ECG); Portugal: art 17 of Decreto-Lei n° 7/2004 de 7 de Janeiro (Electronic Commerce Law); Spain: art 17 of Ley N° 34/2002, de 11 de julio de 2002, de servicios de la sociedad de la información y de comercio electrónico (Act on Information Society Services and Electronic Commerce); Hungary: Act 153 of 2001 on Electronic Commercial Services and Certain Legal Aspects of Information Society Services, promulgated 24 December 2001; Poland: Ustawa o świadczeniu usług drogą elektroniczną (DZ U 2002 Nr 144, poz 1204) (Law Concerning the Provision of Electronic Services). See debate of national implementations in van Hoboken (n 52) 233ff.

[55] Austrian Supreme Court, OGH 20.09.2011, 4 Ob 105/11m ('the defendant's chosen presentation, which 'cut out' the photographs from the original page, altered the original information to the extent that the photographs were—in contrast to the original page were visible on the screen without a manufacturer's note.').

Unsurprisingly, this situation led many to argue that search engines of various kinds are *not* covered by any of the three liability exemptions and remain subject to national experimentation foreseen by the review clause of Article 21 ECD.[56] In the only CJEU case dealing with the question, AG Maduro in *Google France* suggested, however, the opposite. He was of the view that Article 21 does not exclude application to search engines but only instructs the Commission to see if the potential (in) application of the existing framework needs to be adopted.[57] Based on that, he concluded that:

> In my view, it would be consistent with the aim of Directive 2000/31 for Google's search engine to be covered by a liability exemption. Arguably Google's search engine does not fall under Article 14 of that directive, as it does not store information (the natural results) at the request of the sites that provide it. Nevertheless, I believe that those sites can be regarded as the recipients of a (free) service provided by Google, namely of making the information about them accessible to internet users, which means that Google's search engine may fall under the liability exemption provided in respect of 'caching' in Article 13 of that directive. If necessary, the underlying aim of Directive 2000/31 would also allow an application by analogy of the liability exemption provided in Articles 12 to 14 thereof.[58]

Because the case concerned advertising in the search results and not organic search results, the above text was an obiter dictum, which the CJEU never had to address. However, the Court found that keyword advertising in web search results qualifies as hosting.[59]

In the legislative process surrounding the DSA, the Commission's DSA proposal, they remained entirely silent in this regard, preferring to leave the questions to case law. The European Parliament proposed to add that search engines may qualify as caching services ('as to information included in the results') but also as hosting services (as to 'elements displayed alongside those results, such as online advertisements') on a case-by-case basis.[60] The Council proposed to introduce a new fourth category of liability exemptions for search engines with a regime similar to caching[61]

[56] van Hoboken (n 52), 229 ('Article 21 ECD on the re-examination by the European Commission suggests that search engines [information location tools] and hyperlinks are not covered by the intermediary liability regime of the Directive').

[57] Joined Cases C-236/08–C-238/08 *Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2009:569, Opinion of AG Maduro, paras 133–34.

[58] ibid fn 72.

[59] *Google France* (n 20) para 106.

[60] European Parliament, 'Amendments adopted by the European Parliament on 20 January 2022 on the 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 (COM(2020)0825 — C9-0418/2020 — 2020/0361(COD))' [2022] OJ C336/48, 65

[61] General Secretariat of the Council, '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 – General Approach' (2021) Document 13203/21, art 4 on '"Caching" and online search engines' <https://data.consilium.europa.eu/doc/document/ST-13203-2021-INIT/en/pdf> accessed 1 August 2023.

and expand risk management to 'Very Large Online Search Engines' in the due diligence chapter.[62] The Council's liability exemption proposal was controversial because search engines would suddenly be free from notice and action procedures that are required from hosting but not from caching providers. Moreover, this would have granted them broader immunity than the one existing under the US copyright or current case law concerning the right to be delisted under the General Data Protection Regulation (GDPR).

According to Roche Laguna, the discussions around specific liability exemptions for search engines became a complicated battlefield during the negotiations with opposing and sometimes contradictory interests between creative industries, civil rights associations, and search engines of various sizes and types.[63] At a later point in the negotiations, the Council modified its negotiating position towards a fourth category of liability exemption to that of hosting services and subject to a similar knowledge standard. However, this was rejected by the European Parliament due to concerns about the risks to freedom of expression and information.

The final result is the introduction of the definition of search engines in the DSA, mimicking that of the Platform to Business Regulation, but the liability chapter remains silent on search engines (as did the Commission's original proposal). Search engines are only mentioned as a generic type of intermediary provider that facilitates proper functioning of the internet, that can also benefit from the exemptions from liability, 'to the extent that their services qualify as 'mere conduit', 'caching' or 'hosting' services' (Recital 27). With this, 'very large online search engines' are put at the same level in terms of due diligence obligations as 'very large online platforms', although they do not have one universal exemption.

The situation of search engines is further complicated because today's generalist search engines are composite services that package many different technical activities into one product. However, these technical activities 'source content' differently: a) natural search results consisting of hyperlinks and short excerpts collected from websites on an opt-out basis, b) advertising results designed by advertisers who also select keywords to trigger them, c) suggestions in the search bar resulting from an algorithm that processes the most frequent queries of users, and d) finally, the archival copies of webpages interlinked with some results. To complicate things further, a subset of indexed websites has a more managed relationship with the search engine through various webmaster tools.

Thus, when discussing search engines and their liability exemptions, the discussion must always first clarify which part of the search engine is discussed. There is no single regime for all the above technical functions. Usually, the talks about a 'missing' liability exemption for search engines refer to liability for text indexed in the natural search results. This must be distinguished from *advertising results* that are clearly

[62] ibid 64, Rec 69.
[63] *Interview with Irene Roche Laguna* (n 36).

covered as hosting following *Google France* ruling or *search suggestions* delivered via autocomplete that are not because they are content produced by search engines themselves.[64]

In my view, the historical argument for the positive exclusion of any part of search engines based on Article 21 ECD was never too strong. The legislative history, at best, shows that given the US model, it was not clear how the lack of an explicit category would be applied by European courts. Thus, one cannot infer that search engines were not meant to be covered by the framework *if* the conditions of one of the exemptions are met simply because the review clause of the ECD stressed the need to review the situation. Natural search results store and organise other people's information (excerpts and links). Recipients of search results are the indexed website owners. However, to qualify for the hosting service, Article 3(g)(ii) DSA, as the ECD before, requires 'the storage of information [to be] provided by, and at the request of, a recipient of the service'. The key problem is whether websites that do not opt out of indexing by search bots can be said to 'provide' the information to search engines at the website owners' 'request'. So far, no CJEU case has confirmed this. Nevertheless, in my view, we can say that at least for some natural results displayed in the generalist search engines, there is little reason not to qualify them as hosting (see option three below).

Thus, 22 years after the adoption of the ECD, the attempt to create an explicit liability exemption failed. This outcome creates a lot of uncertainty. Unless the CJEU explicitly addresses the status of natural search results, national case law among the Member States will likely diverge. In contrast to the days of the ECD, the proper classification of natural search results under the DSA carries some immense consequences.

Firstly, proper interpretation determines whether the Member States can create or maintain their specific liability exemptions for search engines or whether they are pre-empted by the full harmonisation effect of the DSA. Secondly, search engines, their users and victims might not know which baseline legal expectations apply. Should providers put in place a notice and action mechanism like hosting providers? Should they send statements of reasons? If so, to whom? Should they then forward those statements of reasons to feed the database to be put in place by the Commission?[65] If natural search results are hosting services, are they also platforms if they disseminate content to the public? Moreover, not all search engines function the same way. Will clarity as to what the classical, big search engines must do also apply to those who do not generate their own index of the internet and only syndicate the indexes of some other search engines? Will these standards also apply to specialist search engines?

[64] German Supreme Court, BGH v 14 May 2013—Case No VI ZR 269/12, paras 19ff; Austrian Supreme Court, OGH 30 March 2016, 6 Ob 26/16s, para 3.3 (rejects liability exemptions).

[65] As Google already does today to the Lumen database; see the Lumen Database <https://www.lumendatabase.org> accessed 1 August 2023.

In my view, the Court has four options.

The *first option* is to deny the applicability of any liability exemptions to natural search results with an argument that the legislature excluded such services through the original review clause of the ECD. Very large online search engines (VLOSEs) would be subject to uniform European due diligence obligations but diverging national liability regimes. However, this will cause difficulties for the DSA because such providers are asked to assure the same level of risk mitigation across the Union even though their liability question would be treated differently. For instance, if Austrian law imposing the conduit regime was respected, the due diligence obligations could hardly request notice-based content moderation to mitigate risks. Not only is this option sub-optimal from the perspective of the EU single market, but it also does not find much support in history.

The *second option* would be to accept that storing and ranking natural search results concerning all websites constitutes the activity of hosting despite search engines dispatch crawlers to collect such information without seeking opt-in. The CJEU would need to recognise that even implicit provision of information by recipients of the service, that is, by not opting out of the industry standard, is sufficient to 'provide' such information at the 'request' of those websites. To date, similar logic was accepted in copyright law, but never for a liability exemption itself.[66] However, even if the Court did this, the question of the provider's neutrality would need to be addressed to provide a complete answer. The additional advantage would be that while the Court would have to see to what extent the content moderation due diligence obligations can be applied to search, they would form a common baseline for the special risk management system foreseen by the DSA. The Court could easily synchronise its reading with the GDPR.

The *third option* would be to limit hosting liability exemption to only websites with more managed relationships with search engines. Some websites proactively submit information about themselves to search engines, sometimes using the provided interfaces, such as webmaster tools. In these cases, there is explicit provision and request to store information in some form. While this would only solve the problem of search engines' liability for some websites, arguably, it would apply to the key parts of the digital ecosystem. It would incentivise search engine providers to treat the content of websites with less-managed relationships differently .

The final *fourth option* would be to liken the search engines to caching. That said, I personally see little reason why storing and sorting content in a quasi-permanent index should be viewed as temporary storage that facilitates access to information. Many hosting services already facilitate access, too, and are not treated as caching. Moreover, if one accepts that caching services should be inherently less involved in

[66] German Federal Supreme Court, BGH v 29 April 2010—I ZR 69/08 (*Vorschaubilder)*.

modifying the information compared to hosting, natural search results could easily lose such exemptions due to a lack of neutrality, exemplified by some national case law cited above.

In my view, the second option seems possible, and the third option seems safe. If the Court recognised natural search results as hosting, as some courts already do,[67] the DSA would gain a better grip on the services. Not only do many search engines already operate under hosting's notice and takedown choreography, but some other areas of EU law already impose liability on them, which seems to replicate (in effect) the hosting exemption model. In EU copyright law, it was found that placing unauthorised content in the natural results implicates the search engine only upon notification[68] and that search engines should not be subject to general monitoring.[69] Even in right-to-be-delisted cases under the GDPR, the CJEU accepted that requests trigger the obligations.[70] The decisions concerning search engines often emphasise their importance for the health of the digital ecosystem and the freedom to convey and receive ideas within it.[71] According to *AG Maduro*, search engines are neutral[72] and some national courts already argued that such results are not perceived as the search engine's own content.[73] Finally, this option would be in line with the US copyright regime and the way how many companies already operate even in other areas that are clearly outside of the liability exemptions.[74]

If the Court were to decide in favour of the first option, the Court would find it hard to avoid harmonising law through due diligence obligations. For instance, the rules prescribing mitigation of risks, including preventing over-removal, can hardly achieve the same effects in two countries that expose the search engine to two different liability schemes: knowledge-based standards or stricter forms of liability. The Court will, therefore, have to consider how the accountability rules and the need for their effectiveness might indirectly shape the liability frameworks that are not explicitly harmonised. For instance, it can consider the pre-emptive effect of rules, such as Articles 34–35, on the national liability frameworks.

Even more so than in other areas, the CJEU's interpretation of this will be key. I will show in the due diligence chapters (Part III of this book) that applying

[67] The most recent example is when the Italian Supreme Court found that search engines are, in principle, eligible for the hosting liability exemption (Italian Supreme Court, Cass, 8 June 2022, n 18430) and hence should honour valid notices to be exempted from liability.

[68] German Federal Supreme Court, BGH v 15 September 2017—I ZR 11/16 (*Vorschaubilder III*) paras 63, 67.

[69] ibid para 62; this is part of the assessment in InfoSoc Directive, art 3.

[70] Case C-136/17 *GC and others v CNIL* ECLI:EU:C:2019:773, para 47 ('the prohibitions and restrictions in Article 8(1) and (5) of Directive 95/46 and Articles 9(1) and 10 of Regulation 2016/679 … can apply to that operator only by reason of that referencing and thus via a verification, under the supervision of the competent national authorities, *on the basis of a request by the data subject*') (emphasis mine).

[71] For instance, in Germany: German Federal Supreme Court, BGH v 27 February 2018—VI ZR 489/16 (defamation, for results in SE), paras 32–33 and 35–36; *Vorschaubilder III* (n 68) paras 54–56 and 60. In the Dutch case law, Hoboken reported a similar hosting-like regime in 2012, van Hoboken (n 52) 235.

[72] *Google France (Opinion of AG Maduro)* (n 57) para 144.

[73] German Federal Supreme Court, BGH v 27 February 2018—VI ZR 489/16, paras 28–29.

[74] BGH v 14 May 2013—Case No VI ZR 269/12 (n 64) (notice-based liability for defamation even though suggestions are not covered by a liability exemption); similarly, in BGH v 27 February 2018—VI ZR 489/16 (n 73) para 36.

content moderation safeguards is crucial for many of the existing problems across a wide range of areas. While the DSA's content moderation chapter needs some adjustment to reflect the specifics of search engines, the problem is not dissimilar from the Court's task of adjusting the data controller responsibilities of search engines in data protection law.

7.6 Liability Exemptions Overlaps and Voids

Some providers of technical services were not included among the covered relevant technical activities by the EU legislature's choice. National laws can offer them additional liability exemptions or make them subject to different due diligence obligations; however, they must first rightly establish that the DSA does not regulate such services. This is more easily said than done, as seen in the example of search engines.

Moreover, one product might sometimes fall under more than one liability exemption, and such an *overlap* of exemptions can trigger a potential clash.

Firstly, some services might be concurrently described as 'storage' (hosting) and 'transmission' (conduit).[75] The typical case is messaging apps—cloud-based apps are hosting, while cloudless apps are conduits (Chapter 9). Secondly, sometimes 'access' could rival 'caching', such as in the case of CDNs. In both situations, if two exemptions cover the same activity, the CJEU will have to decide which of the two exemptions should be preferred. As discussed in the section about mere conduits, the temporal character of storage should be able to resolve many of these cases (ie more permanent storage leading to hosting). Similar considerations could be employed between the overlap of mere conduits and caching (see, respectively, Articles 4(2) and 5(1)(c) DSA).

In contrast to an overlap, a more frequent situation encountered is that of bundled and composite services.

Bundled services offer separable services in one consumer bundle. For instance, in the same product package, telecommunication companies can provide conduit services (eg the Internet connection, a public wi-fi hotspot), caching services (eg to ensure smooth streaming), hosting services (eg cloud space for private use), along with other retransmission of editorial content (eg TV 'on-demand'). The liability exemption under Articles 4–6 DSA only cover the particular services covered under such category, but not the others (eg TV on demand). In most cases, it is irrelevant that such services are offered together. This differs from what I call *composite* services, such as search engines—where several technical functions are integrated into a single service. The DSA tries to surgically separate the technical functions of such services for the purposes of liability exemptions. Thus, two different regimes can be applied if one can easily separate advertising from autocomplete results.

[75] The CJEU very indirectly touched on the issue in *Google France* without providing much guidance. *Google France* (n 20) para 111.

However, accountability under the DSA operates with a broader notion of the 'service' that includes the entire separable user experience. Thus, an online platform might be accountable for respecting due diligence obligations for product features that do not qualify as hosting if they are built as inseparable components of the same business product (Chapter 9.2.2). This means that for due diligence obligations, even own editorial content integrated with non-editorial content can become regulated to some extent (eg the sale of own goods and those of others; the publication of one's own articles along those of the users).