Information Law and Policy Lab

Information Law and Policy Lab x ACM

Group Chats, Public Platforms?

Classifying Hybrid Services under the Digital Services Act

Amsterdam, juli 2025

This policy paper was written by Jasmine Tona, Kiki Beckers, and Raoul van de Geer, as part of the Glushko & Samuelson Information Law and Policy Lab (ILP Lab) at the Institute for Information Law (IViR), University of Amsterdam.

At the ILP Lab, students develop research-based policy proposals under the supervision of IViR researchers, aiming to advance the protection of fundamental rights and freedoms in the field of European information law. This policy paper was produced in response to the request of the Netherlands Authority for Consumers and Markets (ACM). The ACM requested the ILP Lab to perform a study and give advice regarding the definition of an online platform service under the DSA. We thank Ot van Daalen (IViR) for his guidance throughout the research process.

This paper reflects the views and analysis of the authors

Executive Summary

Group Chats, Public Platforms? Classifying Hybrid Services under the DSA

This research was conducted by the Information Law and Policy Lab in response to the request of the Dutch Authority for Consumers and Markets (ACM). It explores the regulatory uncertainty under the Digital Services Act (DSA) surrounding hybrid and group-based digital services such as Telegram, WhatsApp, and Facebook, which blur the lines between private messaging and public dissemination.

Context & Research Question

The central research question addresses under what conditions group-based hosting services can be classified as online platforms within the meaning of the DSA - a classification that triggers enhanced due diligence obligations, such as prioritising reports from trusted flaggers.

Legal Ambiguity

The study identifies a core legal ambiguity in Recital 14 DSA, which exempts interpersonal communication services from the platform definition, while including services that disseminate content to the public. It examines two competing interpretations of this recital:

- **a strict reading**, focusing on technical access control and sender-defined audiences, and
- **a flexible interpretation**, based on the service's actual function, public reach, and societal impact.

Key Findings

The research draws on EU legal frameworks including copyright law, telecommunications law, and the Regulation on Terrorist Content Online, as well as relevant CJEU case law and legislative history. Expert interviews with academics and regulators add insight into current enforcement practice and doctrinal uncertainty.

Key findings include:

- The flexible, functional interpretation of "dissemination to the public" aligns more closely with the DSA's goals and with related EU case law (e.g., copyright jurisprudence).

- Platforms that enable large-scale content sharing, even via semi-closed groups or invite links, may functionally operate as public fora and thus fall within the DSA's scope.
- The distinction between hosting services and online platforms depends not only on form but also on context, including audience reach, access control, and content persistence.
- A lack of harmonised interpretation among EU Member States risks legal fragmentation, forum shopping, and inconsistent enforcement.
- Proactive classification by national authorities (such as the ACM) is legally defensible but may carry political or legal risks if diverging from other EU regulators.

Regulatory Implications

The report does not provide normative recommendations but instead offers a legally grounded framework for assessing whether group-based services fall within the DSA's definition of online platforms. The findings support a function-oriented approach that considers the realworld design and impact of digital services.

Table of Contents

Chapter 1 Introduction and Problem statement

The Digital Services Act (hereinafter: DSA), which is fully applicable as of February 17, 2024, constitutes a significant advancement in the regulation of digital services within the European Union.[1] It builds upon and modernises the legal framework introduced by the E-Commerce Directive (hereinafter: ECD) of 2000. While the ECD laid the foundation by establishing liability exemptions (safe harbours) for intermediary service providers (such as those offering hosting, caching, and mere conduit services) the evolving digital landscape has revealed the need for a more robust and responsive regulatory approach. The rise of online platforms, coupled with the growing prevalence of disinformation, hate speech, and other forms of illegal content, has underscored the urgency of enhanced oversight. Rather than replacing the ECD, the DSA complements and extends its core principles by introducing updated responsibilities and liability regimes tailored to today's online environment.

A key feature of the DSA is the classification system for digital service providers, which directly determines the scope of their obligations and potential liability. Providers with greater reach and societal impact are subject to stricter due diligence requirements. These may include riskbased content moderation duties, provided they remain consistent with the prohibition of general monitoring, as reaffirmed in Recital 30 of the DSA.[2] The overall aim is to foster a safer, fairer, and more transparent digital ecosystem across the EU.

1.1 Problem statement

While the DSA provides a comprehensive legal framework for regulating intermediary services in the EU, its practical enforcement presents significant challenges - particularly when it comes to hybrid or borderline digital services that do not clearly fall within the categories of "hosting service" or "online platform." A key legal uncertainty concerns the classification of groupbased or messaging-based services, such as Telegram groups or WhatsApp Channels, under Article 3(i) DSA.

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[2] Recital 30 DSA clarifies that providers of intermediary services should not be subject, either in law or in practice, to a general monitoring or active fact-finding obligation. This does not preclude specific monitoring obligations pursuant to lawful orders by competent national authorities, in line with Union law and the conditions set out in the Regulation.

Public-facing features such as Telegram channels or Facebook pages likely qualify as online platforms, given their broad audience reach. However, services with both public and private functionalities (such as large group chats on WhatsApp or Facebook) create ambiguity. These platforms often combine interpersonal communication with mechanisms for mass dissemination, blurring the boundary between private messaging and public communication. As a result, classification may need to be made at the level of functionality rather than by service as a whole. This distinction is not merely formal: the classification directly determines whether stricter due diligence obligations apply, such as the obligation to prioritize reports from trusted flaggers. The core difficulty lies in interpreting "dissemination to the public" as described in Recital 14 DSA. It remains unclear at what point closed groups transition into public fora, thus triggering platform-level obligations.

A further challenge arises from the lack of harmonized interpretation across EU Member States. Diverging approaches to Recital 14 risk legal fragmentation, uncertainty for crossborder platforms, and potential regulatory arbitrage. Services may intentionally design access controls to avoid classification as “public,” even while enabling large-scale content sharing in practice. Moreover, the DSA’s current focus on public content creates an enforcement gap. Closed groups (despite functioning as de facto public spaces) are often excluded from oversight. This limits transparency, complicates intervention, and raises questions about whether due diligence obligations should extend to large semi-private communities.

This research therefore investigates under what conditions certain hosting services, particularly those with large group-based functionalities, should be considered as disseminating content to the public under the DSA, and what legal and enforcement implications arise if national regulators, such as the ACM, adopt divergent interpretations in the absence of EU-wide harmonization. The above problem statement leads to the following main question:

"Under what conditions can sub-services of hosting providers be classified as online platforms within the meaning of the Digital Services Act?

To answer this main question, the research is structured around the following sub-questions:

1. What are the legal criteria for distinguishing between a hosting service and an online platform under the DSA, and how do the corresponding due diligence obligations differ?

2. How is the concept of "dissemination to the public" interpreted in relevant EU legislation and case law, and what factors determine whether content reaches a public audience?
3. How do current digital (sub)services (such as Telegram, WhatsApp, and Facebook) function in practice, and how do their public or semi-public features align with the DSA's definitions and obligations?

The structure of this report follows the sub-questions: Chapter 2 addresses Sub-question 1, Chapter 3 addresses Sub-question 2, and Chapter 4 addresses Sub-question 3.

1.2 Methodology and scope

This research adopts a doctrinal legal methodology, focusing on the analysis and interpretation of primary EU legal sources, particularly the DSA. Additional relevant instruments, such as EU copyright law, telecommunications law, and the Regulation on Terrorist Content Online, are examined where they offer interpretive guidance. Case law from the CJEU is also considered.[3] To complement the legal analysis, interviews were conducted with academic and regulatory experts in the field of digital services. These qualitative insights offer practical perspectives on enforcement and interpretation under the DSA. In addition, a comparative assessment of platforms such as Facebook, Telegram, and WhatsApp illustrates how different services operate in practice and how their features align (or conflict) with the legal definitions and obligations under the DSA.

The study is limited to EU law and enforcement frameworks. Non-EU examples may be referenced for context but do not form part of the core analysis. Technical elements such as encryption are discussed only where they carry legal relevance. By combining doctrinal research, expert input, and practical platform analysis, the study provides a grounded exploration of how hybrid digital services may fall within the DSA's classification system.

[3] In examining related areas of EU law, this research seeks to identify how certain terms and principles have been interpreted or developed beyond the DSA. Such cross-referencing enables a deeper and more coherent understanding of the legal language within the DSA, by drawing on established interpretations and analogies from other legal fields.

Chapter 2 Legal Framework DSA

The DSA introduces a layered framework for regulating digital services. A key distinction is made between hosting services and online platforms, with different legal obligations depending on the type of service. This chapter examines the definitions and legal criteria of both concepts under the DSA, the relevant factors for differentiation, and the differences in due diligence obligations.

2.1 Definitions under the DSA: Hosting Service and Online Platform

The DSA defines a hosting service as an information society service that consists of storing information provided by a user (recipient) at their request. In other words, the service functions as a repository for user-generated content.[4] Examples include web hosting, cloud storage, or similar services. The Dutch text states: *"a service that consists of the storage of information provided by the user of the service, at their request."*[5]

Recital 29 of the DSA emphasizes that the classification of a service as a hosting service depends primarily on its technical functionality. Specifically, it requires that users voluntarily provide content, which is subsequently stored on the service's servers. This storage must be persistent or accessible on demand, rather than being merely temporary or cached. Furthermore, the stored content must be retrievable by third parties, extending beyond simple technical delivery between sender and recipient.

This technical qualification forms a necessary precondition for further assessment under Article 3(i) DSA. In other words, a service can only qualify as an online platform if it is first considered a hosting service. Services that merely act as conduits (such as messaging apps with transient caching) fall outside this definition.

Under the DSA, an online platform is defined as a specific type of hosting service that not only stores information at a user's request but also disseminates this information to the public at the user's request.[6] The crucial aspect is the public accessibility of the content posted by users. The DSA describes online platforms as, for instance, social networks or online marketplaces where user-generated content is widely accessible. The Dutch explanation states: *"Online platforms,*

[4] Art. 3 DSA, via eu-digital-services-act.com

[5] BIPT, *DSA: aanbieders van online tussenhandelsdiensten*, via bipt.be [6]

Idem.

such as online marketplaces, app stores, or social networks, not only store information provided by users but also publicly disseminate it, i.e., make it available to potentially all users.[6]

2.2 Relationship between Hosting Service and Online Platform

An online platform is a subcategory of hosting services under the DSA.[8] The distinction depends on whether the service disseminates information to the public. Criteria and relevant factors for the distinction:

- **Public accessibility:** There must be a provision of information made available to an indefinite, potentially unlimited number of people. Recital 14 of the DSA clarifies that "dissemination to the public" means that the information is easily accessible to the general public without any further action required from the user who uploaded the information. It concerns availability to potentially all users of the service. [7] The requirement for individuals to register or become a member of a platform does not, in itself, prevent the information from being considered publicly disseminated, provided that registration or admission happens automatically and without selection by, for example, an administrator. A post on a public social network or a product listing on a marketplace is aimed at an unlimited audience, whereas a message in a closed chat group is not. Recital 14 further clarifies that the information must be accessible to a potentially unlimited number of recipients, and that the sender of the content must not determine the audience.
- **Interpersonal communication vs. publication:** Services that enable direct interpersonal communication (e.g., email, private messaging) where the sender controls recipients are excluded from the definition of online platforms.[10] Their audience is limited and predetermined.
- **Core functionality vs. ancillary functionality:** Public dissemination must be a core, not incidental, part of the service. As Recital 13 explains, limited public features such

[6] Europese Commissie, *DSA Transparency Database – Questions and Answers*, via digital-strategy.ec.europa.eu [8] Recital 13 DSA.

[7] Europese Commissie, *DSA Transparency Database – Questions and Answers*, via digital-strategy.ec.europa.eu [10] Recital 14 DSA.

as comment sections on news websites do not transform such services into online platforms, provided that public dissemination is not central to the service's main function.

- **Technical integration and avoidance:** The DSA prohibits circumvention of regulatory obligations through technical integration. Public dissemination features embedded in otherwise private services cannot avoid qualification as an online platform if they functionally serve a public audience.[8]
- **Infrastructure vs. publication:** Recital 13 clarifies that infrastructure-based hosting services (such as cloud computing or web hosting that purely operate in the background for a website or application) are not considered online platforms when they do not themselves make information publicly available.

In summary, a hosting service is considered an online platform as soon as, and to the extent that, it actively functions as a public forum for user-generated content. Context and functionality are key. In borderline cases, the design and setup of the service will be examined: if the service is aimed at broadly sharing user content (as is the case with social media, marketplaces, or content-sharing platforms), it qualifies as an online platform. If the service is limited to storage or transmission without public access (such as a private cloud, email server, or purely technical background hosting), it remains a hosting service.

2.3 Due diligence obligations: hosting service vs. online platform

The DSA introduces a layered system of due diligence obligations, with the intensity of requirements depending on the classification of the service. Hosting services (Art. 3(g) DSA) are subject to a basic level of obligations, including:

- A notice-and-action mechanism (Art. 16 DSA), which requires providers to act upon receiving substantiated notifications of illegal content;
- A duty to provide reasons when content is removed or access is restricted (Art. 17 DSA);
  - and an obligation to notify authorities of any suspicion of serious criminal offences (Art. 18 DSA).

Online platforms, as a public-facing subcategory of hosting services (Art. 3(i) DSA), are subject to heightened due diligence requirements due to their societal impact. The most relevant enforcement- related obligation in this context is the duty to give priority to notices submitted by trusted flaggers (Art. 22 DSA). These are entities officially designated by national Digital

[8] 8 Art. 3 DSA.

Services Coordinators, whose notifications are presumed to be accurate and must be processed with priority by online platforms. This obligation creates a clear enforcement threshold: only services that qualify as online platforms under the DSA are legally required to implement trusted flagger mechanisms. As a result, the classification of a service as an online platform, particularly in borderline cases involving large group functionalities, has direct implications for the visibility, speed, and effectiveness of unlawful content removal.

By contrast, hosting services that do not meet the threshold of public dissemination are not subject to the trusted flagger regime. This significantly limits regulatory oversight in semipublic or hybrid services unless they are explicitly brought within the platform definition.

Summary: Hosting services face limited obligations under the DSA. Only online platforms must comply with trusted flagger rules. As such, the classification as a platform or not has major enforcement consequences.

Table 1: Comparative overview of hosting services and online platforms as defined in the DSA

Characteristic	Hosting Service	Online Platform
Definition	Storage of information at the request of users.	Storage and dissemination of information to the public at the request of users.
Public accessibility	Not required; content can be private or limited-access.	Required; content is made publicly available.
Examples	Cloud storage (Google Drive, Dropbox), web hosting (AWS).	Social networks (Facebook, Twitter), marketplaces (eBay, Vinted), video platforms (YouTube, TikTok).
Interpersonal communication	Possible, but not required.	Interpersonal communication where the sender controls the recipients, such as private messaging, is excluded from the definition of an online platform under the DSA.
Core functionality	Storage and technical service provision.	Active dissemination of user content to the public.
Ancillary functionality	May include limited public sharing (e.g., comment sections), but this is secondary.	Public dissemination is an essential part of the service.

Technical role	Purely storage, without active distribution.	Facilitates and promotes public content distribution.
Infrastructure vs. publication	May operate in the background (e.g., cloud providers, web hosts).	Directly involved in making content visible to a large audience.

Chapter 3 Dissemination and Communication to the public

In order to address the main question, this section will explore the relevant legal frameworks and case law that shape the interpretation of this concept within EU law. Before answering the question of whether a hosting service can be considered a private service or whether it disseminates information to the public, a legal analysis is required based on the various current regulatory frameworks and relevant case law. The concepts of 'dissemination' and 'communication' to the public are addressed in various legal sources, such as the DSA, copyright law but also telecom law and, for example, the Regulation on Terrorist Content.

3.1 Copyright Law

To understand how the term "dissemination to the public" in the DSA should be interpreted, it is helpful to look at the established concept of "communication to the public" in EU copyright law. While these legal frameworks serve different purposes, they both ask the same fundamental question: does content reach a sufficiently broad audience to justify legal obligations?

Under Article 3(1) of the Copyright Directive, authors have the exclusive right to make their works available to a public. According to the CJEU, this concept includes not only direct sharing (e.g. broadcasting), but also passive or technical facilitation (such as hyperlinking, uploading, or indexing) so long as it makes content available to others. Actual access or engagement by users is not required. The decisive factor in these cases is whether a public is reached. The CJEU has developed this notion across a large body of case law, and the following key features can be distilled:

- **An indeterminate and fairly large number of people**
  The audience does not need to be precisely defined; what matters is that it goes beyond a fixed or limited group and remains open-ended in composition.[9]
- **A group that can be reached sequentially, not just simultaneously**

[9] See: *SGAE v. Rafael Hoteles* (C-306/05), where the CJEU held that hotel guests watching television in their rooms constituted a communication to the public. The Court emphasized that the guests formed an indeterminate group of persons, changing over time and lacking mutual personal connections.

Access can occur over time. It is enough that the group remains open and that content is available to new members as they join.[10]

- **A group that exceeds a de minimis threshold**
  The Court has set a low bar for how large the group must be. Importantly, this includes both simultaneous and successive access, meaning even one-by-one downloads or views can qualify if the overall audience is broad.[11]
- **A group with easy joinability or automatic entry**
  If users can join the group with little effort or are automatically granted access, it strengthens the qualification as a public.[12]
- **A group that is not limited to family or close friends**
  Private or intimate circles are excluded. But any group without strong mutual ties (such as large, loosely structured messaging groups) is considered public.[13]

These criteria are especially relevant when evaluating messaging-based services such as Telegram or WhatsApp. The CJEU has recognized that even closed digital environments may constitute "a public" if they are sufficiently large, easily accessible, and allow ongoing participation, regardless of whether the group is publicly listed. This understanding is crucial under the DSA, where the notion of "dissemination to the public" functions similarly to its role in copyright law. It helps distinguish between passive content storage and active distribution mechanisms.

If certain Telegram groups meet the public threshold in copyright terms, it becomes difficult to argue that they should be exempt from the DSA's platform obligations, particularly when they

[10] See: *Tom Kabinet* (C-263/18), where the CJEU ruled that offering eBooks for download may amount to a communication to the public, even if users access the content individually over time; the key factor was the availability to an undefined group. Contrast this with *Del Corso* (C-135/10), in which a dentist playing music in his waiting room was not considered to be communicating to a public, as his patients were seen individually and did not form a large or open audience.

[11] See *Phonographic Performance (Ireland) Ltd v. Ireland* (C-162/10), where the CJEU confirmed that even small audiences may constitute a public, provided the group is not negligible and access is not private. See also *Del Corso* (C-135/10), where the Court reiterated that the audience must exceed a minimal threshold, though not necessarily be large - the "de minimis" standard is low and depends on the specific context.

[12] See: *Stichting Brein v. Ziggo BV (Pirate Bay)* (C-610/15), where the Pirate Bay facilitated access to copyrighted works. Users could join and access content with ease, supporting the idea that accessibility (especially when technically enabled) is central to the "public" concept.

[13] See: *Football Association Premier League (FAPL) v. QC Leisure (C-403/08 and C-429/08),* The Court held that showing football matches in a pub was a communication to the public, as the audience (pub-goers) was not a private circle of acquaintances but an open and paying public. Similarly, in *SGAE v. Rafael Hoteles (C306/05),* the Court confirmed that a transient and unrelated group, such as hotel guests, does not qualify as a private or familial circle.

enable large-scale dissemination of user-generated content. In digital contexts, the bar for what qualifies as "public" is relatively low. Therefore, even semi-private or closed groups can fall within the DSA's scope if they exhibit features of mass accessibility and communication.

By contrast, a dissemination to the public appears to be a broader and more general term that appears in several areas of EU legislation, including the DSA and telecommunications law. Unlike the more specific copyright-focused term "communication", dissemination refers more generally to the act of making information, content, or data available to a wider audience. In the context of the DSA, dissemination relates to online platforms that spread information to the public, with an emphasis not on copyright, but on issues such as transparency, content moderation, and societal impact. While the CJEU has not yet extensively addressed this concept in case law, the focus of "dissemination" lies more on the factual act of spreading content than on legal questions of copyright or public access rights.

The CJEU's copyright jurisprudence offers a helpful, technology-neutral framework for assessing public dissemination. Applying a similar logic under the DSA suggests that hybrid or closed services, when scaled to thousands of users and easily accessible, should not be exempt. Instead, factors like technical openness, user growth potential, and content persistence should guide classification. This would ensure that services with significant societal impact remain subject to appropriate regulatory scrutiny under the DSA.

3.2 Telecommunications Law

Under telecommunications regulation, there is a clear definition of interpersonal communication services: services that enable direct, interactive communication between a finite number of natural persons, selected by the sender. If this definition is met, one can legally argue that there is no online platform in the sense of the DSA, as there is no communication with the public.

According to Article 2(4) of the European Electronic Communications Code (Directive (EU) 2018/1972), an interpersonal communication service (ICS) is defined as: "a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication

merely as a minor ancillary feature that is intrinsically linked to another service." Interpersonal communications services are further subdivided into:

Article 2(6) and 2(7):

- **Number-based interpersonal communications services**: services that connect with public numbering resources (e.g. phone numbers); and
- **Number-independent interpersonal communications services**: services not reliant on numbering plans, such as most messaging apps (e.g. WhatsApp, Signal).

Telecommunications law thus provides a basis for interpreting such services and developing legal criteria to classify them. The relevant definition is set out in the European Electronic Communications Code (EECC). Moreover, this interpretation should be situated within a broader legal context that includes fundamental rights. For instance, Article 5(1) of the EPrivacy Directive explicitly safeguards the confidentiality of communications, ensuring that private communications remain protected. This aligns with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, which guarantee the right to respect for private life and the protection of personal data, respectively.

If a communication service falls under these protections, it implies that the information is not intended for public dissemination and therefore should not be classified as public communication or as an online platform.

3.3 Terrorist Content Regulation

Both the European Regulation on Terrorist Content Online (hereinafter: TCO) and the DSA explicitly acknowledge the dual role of hosting service providers within the digital ecosystem: on the one hand, as facilitators of public communication, and on the other, as potential channels for the dissemination of content, including illegal and terrorist propaganda.[14] This tension between facilitating open discourse and addressing the misuse of hosting services is central to the EU's regulatory approach to online intermediaries.

The use of the term "dissemination to the public" serves in the TCO as a triggering criterion: content must be made publicly accessible, or intended to be, to fall within the scope of the

[14] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (TCO).

regulation. The same principle is implicitly embedded in the DSA, where the public character of content and the platform's role in its dissemination are central to assessing risk, responsibility, and the application of notice-and-action procedures (see e.g., articles 3(g), 14, 16, and 34-35 DSA).

In many respects, the DSA builds upon the normative framework established by the TCO.[15] Whereas the TCO specifically targets the prompt removal of terrorist content (within one hour, Article 3 TCO), the DSA provides a general framework for addressing both illegal and harmful content, while maintaining a similar focus on the role of hosting services in the public dissemination of information. Moreover, both instruments underscore that trust in digital services depends significantly on platforms' ability to prevent misuse, without compromising the open nature of the internet.

[15] See, for example, the definition of dissemination to the public in Article 2(3) TCO and Article 3(k) DSA; in both regulations, Recital 14 is nearly identical in wording.

Chapter 4 Strict vs. Flexible Approach

This chapter addresses the core legal issue at the heart of this project: whether large group chats should be classified as online platforms under the DSA. While these groups can enable mass dissemination of user-generated content, they may still be excluded from platform obligations due to a narrow reading of Recital 14. This chapter examines the two leading interpretations of that recital, one strict, the other more functional, and evaluates which better aligns with the DSA's broader legal and policy framework.

4.1 Strict interpretation (Strict, literal reading of Recital 14)

One interpretation of Recital 14 of the DSA maintains a formal distinction between interpersonal communication services and online platforms. Legal scholars such as Sara Eskens have supported this view, which emphasizes the need to safeguard privacy and the confidentiality of communications by excluding messaging apps from platform-level obligations.

Under this reading, group chats on services like WhatsApp fall outside the DSA's platform definition because they do not qualify as hosting services under Article 3(i) (see chapter 2.1). Messages in such chats are stored only temporarily to facilitate delivery, without providing users with persistent, on-demand access. Any caching of media is performance-related and does not amount to hosting in the legal sense.[16]

Recital 14 reinforces this interpretation by excluding services where content is shared with a *"determinate group of persons identified by the sender"*.[20] WhatsApp group chats typically meet this criterion: users are manually added, access is controlled, and the sender determines who receives the message. Even large groups are still considered private, if there is no open or automated access mechanism. A key element in this view is the role of invite links. While such links can be shared publicly, the technical structure of the service remains the same. Access is granted by the group administrator, not the platform itself. From this perspective, the public sharing of a link does not turn a private communication into a public dissemination. Imposing

[16] S. Eskens 2025, '*Public or private communication? Categorising WhatsApp's and Telegram's group chat and channel functionalities under the DSA*', p. 8. [20] Recital 14 DSA.

obligations based on user behaviour, rather than service design, would blur the legal boundaries drawn by the DSA and introduce unrealistic compliance expectations for service providers.[17]

The distinction becomes clearer when comparing group chats to channels. WhatsApp channels allow for persistent hosting of content and are accessible to a broad, undefined user base without sender control.[18] In that case, the criteria of a hosting service and dissemination to the public are met, placing them within the DSA's scope. Notably, WhatsApp includes channel metrics in its transparency reporting under the DSA, supporting this classification.

This functional interpretation relies on how the service is structured, specifically, that access to group chats is controlled manually, and messages are only delivered to selected recipients. As long as these are preserved, large group chats are excluded from platform obligations, even if their scale or function resembles that of public forums.

4.2 Flexible interpretation (based on function, impact, and public reach)

Before turning to the flexible reading, it is important to recall that the legal debate extends beyond the interpretation of "dissemination to the public." Scholars like Sara Eskens argue that certain messaging-based services (such as large WhatsApp group chats) do not even meet the threshold of a *hosting service* due to the temporary nature of message storage. In contrast, this section defends a functional interpretation that not only addresses the "public" dimension of dissemination but also emphasizes that large group chats and channels often involve persistent storage and accessibility - meeting both conditions of Article 3(i) DSA.

The flexible reading of Recital 14 rests on a broader legal and policy rationale. Rather than focusing solely on technical design, such as whether access is manually controlled, this interpretation assesses whether a service, in practice, enables dissemination to the public. It aligns with the DSA's objective to regulate based on function and societal impact, rather than formal labels or structural features.

Legislative history and teleological interpretation of Recital 14

Recital 14 of the DSA aims to exclude private communication from the scope of platform obligations to protect the confidentiality of communications. In the European Commission's

[17] Eskens 2025, p. 29.

[18] Eskens 2025, p. 20.

original 2020 proposal, it was explicitly stated that interpersonal communication services, such as email or messaging apps, fall outside the Regulation's scope.[18] During the negotiations, it was repeatedly confirmed that private communication is, and should stay private.[19]

However, in the European Commission's original 2020 proposal the Commission explicitly warns that the mere ability to create groups does not imply exemption: group functionality in itself does not make a service "private".[20] This nuance is essential, as it shows that the Commission did not want platforms to hide behind group structures to escape regulation.

Throughout negotiations in Parliament and Council, the wording of Recital 14 was further refined. Parliament, through amendments (IMCO, JURI), clarified that only groups with manual access control (i.e. human selection) qualify as 'closed', while automatic access (such as via open links to public Telegram channels) constitutes public dissemination.[21] These refinements aimed to prevent circumvention of platform obligations through the mere technical use of group functionalities without meaningful access restrictions. In addition, Recital 15 introduced a functional approach by stating that services must be assessed per functionality. Public-facing components of hybrid services (such as Telegram) fall under the DSA, even if the service also offers private messaging.

The final wording of Recital 14 includes a clear reference to "services through which information is provided via public groups or freely accessible channels" as potential online platforms. This clause was introduced late in the legislative process, indicating a deliberate effort to prevent large public services such as Telegram from escaping regulation.[22] Denmark noted that extremist groups increasingly use closed groups or channels on platforms to reach large audiences. It urged that the boundary between private and public communication be clearly defined and that the dissemination of content via such (apparently closed) groups or channels should not fall outside the scope of the DSA.[23] The use of the term "channels" strongly suggests that Telegram Channels were explicitly considered. This confirms the intention to exclude such public functionalities from the Recital 14 exemption.

[18] Recital 14 DSA.

[19] Council, WK 9435/2021 INIT, DK Comments on DSA proposal, 14 July 2021, p. 6.

[20] COM(2020) 825 final, d.d. 15 december 2020.

[21] Amendment 14,EP, JURI Opinion on DSA proposal (COM(2020)0825), 2020/0361(COD), 11 Oct 2021.

[22] Recital 14 DSA.

[23] Council, WK 9435/2021 INIT, DK Comments on DSA proposal, 14 July 2021.

Key EU policymakers supported this position. Rapporteur Christel Schaldemose publicly referred to Telegram as a hybrid platform and made clear that its public-facing components should be regulated. Commissioner Thierry Breton likewise emphasized that the DSA's purpose is not to interfere with private communication, but to strengthen oversight over services that shape the digital public sphere. In a Council document (WK 9435/21), Member States affirmed that "private communication is and should stay - private", while also raising concerns about "very large, closed groups", suggesting that size and de facto accessibility should be taken into account.[24] This reflects a rejection of a strict literal reading in favour of a functional assessment.

To conclude, a functional reading of Recital 14 aligns with EU law and legislative intent. It avoids regulatory loopholes and supports oversight of services that operate as public fora in practice.

Teleological Argument: Preventing Regulatory Arbitrage

A teleological interpretation of Recital 14 confirms that its aim is to protect the private sphere, not to create an unintended exemption for large-scale dissemination services. A strict literal reading would yield undesirable outcomes. For example, a Telegram group with 300,000 members may fall outside the DSA, while a niche forum with just a few hundred users may be regulated. This undermines the DSA's foundational principle of addressing risks based on impact and reach.

This point was also acknowledged during national implementation efforts. The Dutch government noted that "public chat groups on Telegram are likely to fall within the definition of an online platform," reinforcing the idea that reach, not structure alone, should be decisive.[25][26] The flexible interpretation thus avoids regulatory arbitrage, where services evade obligations by maintaining minimal technical access restrictions despite functioning as public

[24] Council, WK 9435/2021 INIT, DK Comments on DSA proposal, 14 July 2021, p. 6.

[25] Dutch House of Representatives, Appendix to the Proceedings 2023/24, no. 1260, Answers by the Minister of Justice and Security to questions by MP Kathmann regarding expose groups and doxing on Telegram, 18 March 2024, available at: https://zoek.officielebekendmakingen.nl/ah-tk-20232024-1260.html (accessed 2 July 2025), p. 3 and 4.

[26] See artt. 1 and 2 DSA.

dissemination tools. Instead, it supports a coherent framework in which the DSA's regulatory aims can be meaningfully enforced.[27]

4.3 Strict v. Flexible Interpretation

The strict reading of Recital 14, based on manual access control and sender-determined communication, excludes large Telegram group chats from DSA platform obligations. However, this interpretation leads to inconsistencies with other areas of EU law and the DSA's own logic. As shown in Chapter 3, EU copyright law recognises that availability of copyrighted content on even semi-closed or automatically joinable groups can constitute a "communication to the public" under Article 3(1) of the InfoSoc Directive. The threshold for being "public" is low. If a group reaches a large, indeterminate audience, even sequentially, it qualifies. Applying a stricter test under the DSA undermines legal coherence of EU law. Moreover, the DSA's purpose is to regulate based on risk and societal impact, not purely technical design. A Telegram group with hundreds of thousands of users clearly shapes the public information space, regardless of how users join. To exclude such groups while regulating smaller platforms would produce irrational results and invite regulatory arbitrage.

A functional, flexible reading, aligned with both copyright doctrine and the DSA's systemic goals, avoids this outcome. It ensures that services which de facto enable public dissemination are treated as platforms, even if they mimic private communication structures.

4.4 Determining Hosting Service Status under the DSA

Before determining whether a digital sub-service qualifies as an online platform under Article 3(1) DSA, it must first meet the threshold requirement of being a hosting service under Article 3(g) DSA. This section applies that technical classification step to WhatsApp and Telegram, which both provide hybrid functionalities combining messaging and broadcasting features.

4.4.1 Telegram

Private chats on Telegram are end-to-end encrypted and stored only temporarily for delivery. These do not meet the definition of a hosting service. Public channels and large group chats, however, function differently:

- Content is uploaded by users (e.g. admins or group participants).
- It is stored on Telegram's servers and can be accessed asynchronously.
- Other users, including non-senders, can view and retrieve the content.

These features qualify Telegram public channels, and likely also large groups, as hosting services under Article 3(g) DSA. This is a precondition for further assessment under Art. 3(i) DSA (platform qualification).

4.4.2 WhatsApp

WhatsApp still offers end-to-end encrypted private and group chats, where messages are stored only temporarily and remain accessible solely to predefined recipients. These functionalities do not meet the technical criteria of a hosting service under Article 3(g) DSA.

The introduction of WhatsApp Channels marks a functional shift: messages are stored persistently on WhatsApp's servers and are accessible to an undefined audience of subscribers. With sender-controlled recipient selection removed and broad accessibility enabled, this feature does meet the definition of a hosting service within the meaning of the DSA.

4.5 Illustrating Inconsistencies Comparing Platform Classifications

To demonstrate the practical implications of the strict versus flexible interpretations of Recital 14, this section presents a comparative table covering a selection of widely used digital services. These platforms, Telegram, WhatsApp, Facebook, were chosen because they operate across the public-private spectrum and feature both messaging-based and community-driven functionalities. Each platform includes sub-services (such as group chats, public channels, or servers) that challenge the binary between interpersonal communication and online platform functionalities. The comparison highlights how similar features can lead to vastly different legal outcomes depending on which interpretative approach is applied.

Note on human selection in large-scale groups

Recital 14 of the DSA excludes services where users are selected by the sender, suggesting a private rather than public form of communication. However, this assumes that admission to a group involves real and meaningful human control. In practice, many large groups allow users to join after simply clicking a confirmation button or answering a basic entry question, without any substantial review by the administrator.

When this process becomes routine or superficial, and the group continues to grow into the thousands or even hundreds of thousands, the distinction between "manual approval" and "automatic access" becomes unclear. Even if a human technically approves each new member, the group may still function as a public forum in practice. This suggests that what matters is not just whether human selection exists in theory, but whether it is genuinely restrictive and effective. If access is essentially open to anyone, the group may still qualify as enabling public dissemination under the DSA, regardless of its formal access design.

Table 2: Consequences Strict and Flexible Interpretation

Platform	Sub-Service	Number of Users	Human Selection	Classification Strict View	Classification flexible view
Telegram	Large Group Chat (manual invite only)	Up to 200,000 members	Yes, users are manually added by the admin; access is clearly restricted and curated.	Not an online platform (sender/admin controls recipient group; access not public)	Possibly an online platform (limited audience with human gatekeeping; lacks public dissemination)[27]
	Large Group Chat (invite link shared publicly)		Technically initiated by admin but join process is automatic and typically uncontrolled; human gatekeeping is ineffective at scale.	Not an online platform (treated as private interpersonal group; sender/admin controls group membership)	Online platform (functionally public forum due to open invite link and large, indeterminate audience)
	Public Channel (broadcast to subscribers)	Unlimited subscribers	No, anyone can subscribe freely; no human selection or review applies.	Online platform (content is broadcast to an indefinite public audience)	Online platform (content is broadcast to an indefinite public audience)

[27] When group admission becomes routine or superficial, e.g. via widely shared links or automatic acceptance, the difference between "manual approval" and "automatic access" may lose significance. Even where a human technically approves each member, the group may still function as a public forum in practice.

WhatsApp	Large Group Chat (near 1,024member limit with invite link)	Up to 1,024 members	Admin creates link or invites users, but links are easily shareable and often lead to open access; limited effective control in practice.	Not an online platform (does not qualify as a hosting service under Art. 3(g) DSA)	Not an online platform (even if group mimics public space, legal qualification as host is lacking)
	Channel (one-way broadcast feature)	Unlimited subscribers	No, any user can follow the channel (one-to-many broadcast)	Online platform (persistent content hosting and dissemination to the public)	Online platform (persistent content hosting and dissemination to the public)
Facebook	Facebook Messenger Group Chat	Up to 250 members	Yes, users are added manually; access is curated, and scale remains small.	Not an online platform (interpersonal communication with sender-defined audience)	Not an online platform (small scale, curated access)
	Messenger Community Chat	Up to 5,000 members	Admin can approve members, but at larger scales this often becomes routine; human control may be nominal.	Not an online platform (manual control, groupbased communication)	Borderline: may qualify if access open or link-based
	Public Page or Open Group	Potentially millions of users	No, access is unrestricted; anyone can follow or join freely.	Yes, online platform (public dissemination without control)	Yes, online platform (broad audience, high impact)

This table shows that the distinction between private and public communication hinges not only on formal access design but also on how restrictive and effective those controls are in practice. As a result, the line between hosting services and online platforms under the DSA becomes increasingly blurred in large-scale, hybrid settings.

Chapter 5 Conclusion and discussion

5.1 Summary of Key Findings

This research was conducted at the request of the Dutch Authority for Consumers and Markets (ACM), in response to the following central question: *"Under what conditions can sub-services from hosting services be classified as online platforms under the Digital Services Act"*. The aim was to determine whether and under what circumstances certain hosting services could qualify as online platforms within the meaning of the DSA, particularly through the lens of the concept of *dissemination to the public*.

To answer this question, we examined the relevant legal frameworks, including the DSA, the TCO, telecommunications law, and copyright law. While the TCO and telecommunications law offer valuable definitional clarity and general context, they proved of limited interpretative use in addressing the ACM's specific legal question. Their main contribution lies in outlining the broader regulatory architecture within which the DSA operates.

In contrast, copyright law, particularly the extensive jurisprudence of the CJEU regarding *communication to the public*, provided more substantial guidance. By drawing parallels between the copyright concept and the DSA's notion of *dissemination to the public*, and by considering the legislative history of the DSA itself, we were able to reconstruct two possible interpretations of this concept. These interpretations differ in scope, but each provides a reasoned path to the conclusion that, under certain circumstances, a hosting service may indeed fall within the definition of an online platform under the DSA.

On the basis of our findings, we conclude that a functional interpretation, which focuses on the actual role played by a service in making content publicly accessible, is the most coherent and operationally useful approach for the ACM. This conclusion does not constitute a normative recommendation, nor was it the goal of this research to advocate for any particular enforcement strategy. Rather, the outcome provides a legally defensible, though not definitive, foundation for further interpretation and enforcement under the DSA. It demonstrates that, while there is a legal basis for such an approach, the matter is not definitively settled, and further clarification, either judicial or legislative, may be needed.

5.2 Implications of National Divergence in Interpretation

If the ACM were to adopt a functional interpretation of *dissemination to the public*, services like Telegram could fall within the scope of the DSA, with potential enforcement consequences. This would allow the ACM to treat these services as online platforms and impose regulatory obligations under the DSA.

However, unilateral adoption of such an interpretation, especially if it deviates from approaches taken by other national regulators, could lead to legal fragmentation across the EU. Divergent interpretations may undermine legal certainty for cross-border services and incentivize forum shopping, regulatory avoidance, or even strategic non-cooperation. These risks are compounded by the DSA's goal of achieving a harmonised internal digital market.

A further concern is the possibility that platforms could respond to enforcement pressure not by changing their practices substantively, but by making technical design changes intended to avoid falling under the DSA's scope. As noted by Sara Eskens in relation to WhatsApp, seemingly minor technical features (such as limited access, user admission controls, or groupbased sharing mechanisms) can be leveraged to argue that content is not disseminated *to the public*, thereby circumventing regulation. Such developments risk weakening the DSA's effectiveness and may force the European Commission to intervene through additional guidance or future legislative refinement. However, such processes take time and may lead to retroactive uncertainty over national enforcement actions.

In sum, while a functional interpretation offers a legally plausible and practically effective route for enforcement, it also carries important risks of inconsistency, circumvention, and legal challenge. These implications must be carefully weighed, particularly in a harmonised regulatory framework such as the DSA, which is designed to ensure uniform application across all EU Member States.

Annex – List of Interviewees

As part of this research, we conducted interviews with the following experts:

- Mr. dr. Sara Eskens — Vrije Universiteit Amsterdam
- Dr. João Quintais — University of Amsterdam / IViR
- Prof. dr. Joris van Hoboken — University of Amsterdam / IViR
- Michiel van Dijk — Senior enforcement official the data and telecom unit at ACM