10 March 2021

ITI Views on the European Commission Proposal for a Digital Services Act (DSA)

Introduction

Digital services play a foundational role in driving innovation and growth in the economy, supporting the smooth operation of digital supply chains and creating market opportunities and access for businesses of all sizes. Policymakers around the world are grappling with real challenges caused by the scale, speed, and complexity of various types of digital intermediaries, the roles they play regarding content and activities online, and in some contexts, their ability to shape public opinion. At ITI, representing all the segments of the tech industry, we understand and recognise the shared responsibility to maintain a safe, inclusive, and innovative online environment.

We support the goals of the European Commission's Digital Services Act to increase legal certainty, clarify roles, and define responsibilities for actors in the online context, i.e. by reviewing and bringing more clarity to the framework. In the following, we provide recommendations for a balanced and proportionate approach that combines regulatory scrutiny with appropriate rights for all actors in the Internet ecosystem.

General Comments

ITI welcomes the DSA and supports its ambition to create a more secure and transparent online space for all actors involved in the online ecosystem by introducing new obligations and rights for different actors in the online sphere. The **differentiation between types of services and their impact** is necessary to create a **level playing field for all actors online** and recognises the diversity of the online ecosystem while ensuring safety online for European citizens. Specifically, **the proposal clearly differentiates between different types of digital intermediaries, such as mere conduit, caching and hosting services providers.** Proportionate and risk-based rules that are targeted to different types of services are especially important when considering that many companies may not have the ability or right (technical, contractual, or otherwise) to edit or manage content.

The proposal also clearly **differentiates between responsibilities for smaller versus larger players**. Proportionality is key to avoid unnecessary burdens and risk stifling innovation and growth of all companies and especially emergent players. While the scale of platforms is an important factor, size alone does not fully reflect the risk inherent to each platform, other factors such as impact, vulnerability of the business model to abuse, and demonstrated systemic exposure to illegal activities/content should also play a role in determining additional specific obligations. Many services already have systems in place to address the needs of their customers and meet expectations of governments and civil societies regarding content moderation. Such systems should be used to inform requirements and obligations should seek to be complementary to these existing systems. Platforms, especially large platforms subject to additional requirements, should maintain the ability to implement these requirements in a way that best reflects the nature of their services, the type of content they make available, and their risk exposure for users on their platform.

Several important provisions leave critical definitions and methodologies to delegated acts. These are too central to the operation of the DSA to be left to delegated acts that are not subject to the legislative process and prevent participation of Parliament and Council as well as other stakeholders. The references to delegated acts in Articles 23, 25 and the general outline in Section 5 and the methodologies they seek to specify should constitute an integral part of the regulation instead.

Relatedly, the **lack of clear definitions** makes it impossible to understand which companies and products will be subject to which requirements. In particular, we believe that the criteria used to define what constitutes a VLOP, how active users are identified, and the additional obligations associated with this status, would need to be defined in the law and must not be left to the Commission to decide via delegated acts. The diversity of the digital ecosystem has also produced diversity of users and companies' interactions with users. Due consideration should be given to how users are counted, including whether it is based on registered users or guest visits.

The Commission's proposed **enforcement framework** resembles existing enforcement structures for other digital legislation, including the General Data Protection Regulation (GDPR), but seems to diverge in several respects. We propose adding more clarity on which authorities can undertake enforcement activities, in what circumstances, and the relevant due process protections, highlighting the need to create clear pathways. The oversight and enforcement regime should not undermine the country-of-origin principle which remains a key pillar to the functioning of the internal market. In addition, we would welcome clarifications on the methodology to calculate fines.

Lastly, given the importance of this initiative, we want to highlight the **need for all stakeholders to be able to feed into the legislative process**. We appreciate the sense of urgency to make progress, though, we urge the co-legislators to take time to get it right.

Specific Commentary on the Proposal

Articles 1-2, 11: Extraterritorial services

We welcome the approach that rules will apply to providers of intermediary services irrespective of their place of establishment or residence, in so far as they provide services in the EU. However, the text of the proposal represents new and distinct challenges if it is to be pursued in the current form. Given the requirement to have a representative in Europe, as well as consideration for the ability of European citizens to interact with content and services based anywhere in the world, a clear set of rules for when a non-EU service must or must not comply with the DSA should be included in the regulation in order to ensure that the DSA reflects the global nature of the digital ecosystem. Another important clarification on the scope of the law is whether "operating in" means the same as "offering services" in Article 2 of the proposal.

Article 2: Definitions

We welcome the clarification in Article 2(g) that illegal content is any content that is not in compliance with EU law or the law of a Member State. It is essential to maintain the principle of what is illegal, regardless of whether it is online or offline.

We also welcome the definition of online platforms, which provides greater certainty for those hosting services that do not store and disseminate information to the public and should therefore not be included in this platform category, such as B2B cloud service or IT infrastructure providers. Indeed, the potential inclusion of these B2B services would not serve the goals of the DSA, particularly where there is no direct link between the cloud service and the online dissemination of goods, services, or content to third parties. Further, a provider of such B2B enterprise or outsourced hosting services would not necessarily have legal access or control over client or user generated data or content. Many businesses rely on cloud infrastructure or IT providers to build applications, platforms or websites, yet the cloud provider is not necessarily intermediating between the business and its customers, particularly when the service in question is of technical nature.

Articles 3-5: Clarifying rules for intermediaries

We welcome the European Commission's focus on restating and clarifying the liability exemptions for mere conduit, caching and hosting providers. However, more clarity on the concrete definitions of entities in Recital 27 would be welcome e.g. defining differences between mere conduit and caching services based on whether information is in transit or stored temporarily. Additional clarity on the differences between hosting services and online platforms would also be welcomed to ensure that a broad interpretation of the concept of "dissemination to the public" does not have unintended consequences. We encourage consistent application across Member States of the concept of actual knowledge in Article 5 as defined by EU case law.

Article 6-9: Safeguarding limited liability and no general monitoring obligation

We welcome the commitment to maintaining a limited liability scheme while providing the much-needed legal certainty that voluntary content screening does not exclude platforms from liability exemptions. We welcome that the Commission underlines that there should be no general monitoring obligations for platforms to screen content on their sites while promoting responsible actions at the same time. We also appreciate that the Commission outlines concrete conditions that Member States need to meet to issue requests addressed to platforms to act against illegal content or to provide certain information. However, Article 6 needs further clarity of what exactly constitutes actual knowledge of illegal content as referenced in Article 5. For instance, where an intermediary service provider has voluntarily reviewed content or activities for a certain type of specific unlawfulness (or for a certain type of specific violation of its community guidelines), the service provider is not necessarily deemed to have knowledge of any other ways in which the reviewed content or activities might be unlawful. ITI continues to recommend this clarification. In addition, we would further welcome a clarification that the protection of Article 6 is extended to voluntary investigations or other activities aimed at detecting, identifying and removing, or disabling access to content that violates intermediaries' terms and conditions, by either automated or non-automated means.

With regards to orders to act against illegal content or to provide information, as specified in Articles 8 and 9, we encourage the proposal to include a list of contacts per Member State or provide alternative ways to simplify intake and prioritisation of such requests.

Article 10: Single point of contact (SPOC)

We appreciate the Commission proposal's goal to establish fast and easy communication between national authorities and service providers. We agree that having formalised and publicised communication channels is the right approach, however we ask for flexibility in implementing this

requirement to account for differences in how companies are internally organised. For example, a single point of contact for both Member State authorities and trusted flaggers may in fact slow down response by the intermediary. Having the option for separate teams dedicated to those stakeholders may make more sense in practice, depending on the volume and nature of notices the intermediary receives. We also believe that flexibility should be implemented when it comes to designating the points of contact in the intermediaries, and companies should be able to designate team members for this role without necessarily having to hire new staff. This SPOC should be available to DSCs, national authorities, and trusted flaggers, but not the wider public, which should use other designated channels for reporting.

SPOCs already exist today in the area of law enforcement, and they have proven to be beneficial for all parties. They help build trust and communication between services and authorities resulting in a far more efficient and streamlined collaboration. For the various SPOCs envisioned within a company, these contacts need to reflect the different teams and workflows that different issues and obligations will be dealt with, and flexibility in designating the single points of contact will be important.

Article 12: Content moderation references in terms and conditions

We are concerned that including information on content moderation in the terms and conditions could impact contractual liability, as acknowledged in recital 38, and create unintended claims for breach of contract under national civil law, in addition to the compliance and sanctioning regime established by the DSA. We believe companies should have the ability to list these separately or that the rationale for including them in the terms and conditions should be further clarified.

We also seek clarifications that the level of detail required under Article 12 is such that will not allow bad faith actors to circumvent intermediaries' content moderation systems.

Article 13, 33: Transparency reporting for illegal content moderation

Transparency is an important aspect of trust in services and businesses on- and offline. The Platform-to-Business Regulation and consumer omnibus legislation provide a helpful legislative framework for identifying effective and efficient transparency tools that help users and authorities. More clarity is needed in the Regulation on what needs to be reported – i.e. take-downs on the basis of a legal order or administrative decision. We also encourage transparency regarding platforms' policies in handling repeat infringers regarding illegal content. There could also be room for more cooperation between online platforms and public authorities to better address issues arising from repeat infringers.

Article 14-15: Notice and action mechanisms

We appreciate the European Commission's goal to provide all users of intermediary services, be they business users or individuals, the ability to make use of effective electronic notice-and-action mechanisms to report illegal content. Legislators should bear in mind that a potential widening of the notice-and-action system could lead to higher volumes and potentially unfounded notices and dilute resources or takeaway focus from more meaningful cases.

Notice formalities are important to help service providers determine the validity of requests. As different types of content may need to be acted upon differently, we caution against an approach whereby a notice that fulfils all formalities necessarily results in actual knowledge (as Article 14(3) appears to suggest). Additional detail may be necessary for platforms to determine the validity of requests and perform swift and proper action. Moreover, the DSA should acknowledge that notices

should be directed in the first instance to the party with the technical and operational capability to take action against specific illegal content. Hosting service providers should have the ability, upon receipt of a notice through the mechanisms described in Article 14, re-direct the notice to the party which has the technical and operational capability to take action. We caution against the publication of all statements of reason in a public database as we believe this would not be proportionate and may not be technically feasible. Legislators should also consider additional guidance for handling repeat offenders and informing customers of illegal product sales.

Article 17: Complaint handling systems

We take note of the Commission's proposal to introduce an obligation for online platforms to set up an internal complaint-handling system against decisions around take-down of content, termination of service provision or account terminations. This is an area of significant ongoing investment by services, as established by the Platform-to-Business Regulation (P2B), and we encourage the Commission to align these requirements.

In order to meet the goal of providing such a recourse system, automated systems may be critical to fulfil this obligation, as automated systems can be more efficient, consistent, and scalable. We therefore suggest that the proposal should focus on flexibility for tools and systems that platforms may use, including enabling automated systems and avoiding specific thresholds for human operators. We also recommend limiting the time frame during which such systems remain available to users, to ensure this obligation does not impose disproportionate costs on service providers.

Article 18: Out-of-court dispute settlement

Out-of-court dispute settlement (OOC) is already available under a number of EU laws intersecting with the DSA, such as the Audiovisual Media Services Directive, the P2B Regulation and the EU Copyright Directive. It is not clear whether additional OOC dispute settlement mechanisms are needed. We urge the Commission to harmonise those requirements, as well as ODR and ADR bodies for business to consumer issues. Any potential new rules on out-of-court dispute settlement (OOC) should avoid prescriptive requirements around the use of alternative dispute resolution. All actors in the process should have the flexibility to respond in a proportionate way to the situation. While OOC can be a viable alternative to Court proceedings and can benefit faster resolution of conflict, there need to be safeguards against frivolous complaints and parties engaged in OOC should commit to its outcome and not launch judicial proceedings in parallel, all while having a symmetric ability to challenge it.

Article 19-20: Trusted flagger schemes

We welcome the Commission's focus on innovative cooperation mechanisms between the different actors involved in detection and takedown of illegal content online. Awarding trusted flagger status should be a joint effort by the platforms, third parties, rightsholders, NGOs and state-backed groups seeking trusted flagger status, as well as the Digital Services Coordinator of the respective Member State, to ensure that expertise and experience is reflected in the process. The trusted flagger scheme should allow a service some flexibility by platforms to select trusted flagger partners and to continue to manage and prioritise notices depending on the urgency or severity of the content within the trusted flagger system. To increase efficiency of the new tool, sophisticated rights holders, with a large IP portfolio and a good track record of accuracy in reporting, should be able to qualify for trusted flagger status to confirm the authenticity of their goods.

The proposed conditions that trusted flaggers must meet are balanced but could use further specification. For example, in the IP context, clarifications would be welcomed on what "organisations of industry" mean in a context where there are trade associations on the one hand, and IPR service providers/ agencies (e.g. REACT) on the other. In addition, the relationship between rights owners and collective rights groups needs to be clarified to be exact in explaining what loss of trusted flagger status of a collective group means for its individual members. As trusted flaggers can be relevant and practical for both IP and non-IP content, it should be explored whether it would be efficient for both online intermediaries and rightsholders if different trusted flagger systems existed for different types of content.

In other contexts, NGOs or state-backed groups promoting safety online might seek trusted flagger status, where safeguards against potential abuse or misuse of notice systems are essential. Further clarification would be useful when it comes to requirements for trusted flaggers to demonstrate expertise and whether they would need to have a point of contact and legal representative within the Member State of the DSC that they register with.

We welcome the possibility to withdraw the trusted flagger status if the trusted flagger continuously submits insufficiently precise, inaccurate or wrong claims, and we believe that this process would benefit from further specification.

Lastly, the new tool being used widely by third parties, rightsholders, NGOs and other groups could lead to a surge in notices and consideration should hence be given to the number of potential trusted flaggers per online platform to ensure that processing of other notices is not slowed down.

Article 21: Flagging serious criminal offences

We support the concept that services should report suspicions of the most serious immediate threats to the life or safety of persons to law enforcement when they become aware of such activity. However, these circumstances need to be very clearly defined. In line with the limited liability framework, we urge that there must not be a general monitoring obligation and platforms should only be required to act if they are made aware of a situation and there is sufficient information to act. Additionally, further alignment with the conditions imposed under the Terrorist Content Online Regulation in that regard would be highly welcome.

Article 22: Traceability of traders (Know-your-business-customer provision)

KYBC schemes can be helpful to combat illegal content online and enhance consumer protection. Many hosting services already conduct background checks of their customers as part of their own trust and security processes. Nevertheless, while we are encouraged by the Commission's effort in exploring traceability, we caution that the proposed obligations may in some areas need to be more clearly defined and proportionality ensured. For example, to the extent Article 22 is aimed exclusively at online marketplaces, this should be made clear. In addition, requiring online platforms to collect information about economic operators under 22(d) could be problematic, given the number of potential parties along the supply chain that this term may cover, and that this information would be required at the time of opening an account. Any approach should be harmonised and based on the collection of typical identifiers, as outlined in the European Commission's proposal, in electronic format.

Article 24: Online advertisement transparency

We acknowledge the Commission's goal to make identification of advertisements easier for consumers online. We note that already many obligations are in place to disclose information on advertisement. It is important that provisions on advertising take into account the reality of all of the advertising models and reflect the often dual roles that platforms play in this space. For example, in many instances, platforms will not have access to the data as they work with third parties.

Article 25: Defining VLOPs

We believe that the criteria used to define what constitutes a VLOP, and the additional obligations associated with this status, would need to be defined in the law and must not be left to the Commission to decide via delegated acts. While we agree that reach and scale play an important role, other factors such as vulnerability of the business model to abuse and demonstrated systemic exposure to illegal activities/content may also be considered when determining whether the additional specific obligations are required.

For example, consideration should be given to the qualities of the service and how the services address serious issues of illegal content. Size is not the only relevant criterion here as often smaller online platforms can also be responsible for the impactful dissemination of illegal content.

The proposed definition basing itself on the number of 45 million average monthly active users needs further specification to explain what constitutes an "active user" for the very different service types covered by the DSA. It should be clear if the 45 million threshold relates to the number of end users of the customers of a hosting provider, or if it relates to the number of direct customers, where the hosting provider stores and disseminates content to the public at the request of a recipient.

A proposed revision of the definition every 6 months creates legal uncertainty that is unhelpful given the significant compliance burden that companies would encounter when falling within the scope of this definition. Instead, we would suggest reassessing the definition at most every 1-2 years. In the same vein, we encourage a grace period for new VLOPs of 12 months before they have to implement the VLOP-specific elements of the legislation. The current timeline of 4 months is too short to set up an effective compliance process. For example, reporting obligations for VLOPs such as reports needing to be submitted every 6 months require some time to get the right processes set up.

Article 26-27: Risk management & mitigation

The Commission proposal foresees that VLOPs need to identify systemic risks stemming from their services in the EU including dissemination of illegal content through them, negative effects on exercise of fundamental rights to privacy, freedom of expression or rights of the child, intentional manipulation of their services with actual or foreseeable negative effect on public health, minors, etc.

Given the far-reaching nature of these obligations and the types of content that would be covered by this, we would welcome more legal certainty through, for example, a definition of what may constitute a systemic risk. We would also urge that VLOPs have flexibility over the mitigation measures that they choose to implement to address those risks, given the differences in their interactions with data and their business models. The proposed provisions have an honourable goal in mind. However, they may not be suitable for all types of VLOPs' activities and should not extend to B2B services. In many instances, in addition, using reporting mechanisms would be more useful than annual analysis to be able to act fast, efficiently, and specific to a particular issue. Standard content moderation procedures could for example detect spikes in illegal products being sold on a

website and the platform could notify the authorities and act accordingly. Policymakers should also be cautious that risk management does not result in inadvertently introducing general monitoring obligations.

Article 28: Auditing

We support the Commission's goal of enhancing transparency of online platforms through the DSA and acknowledge the appropriate role of audits. However, obliging VLOPs to conduct annual independent, external audits and publish findings in an audit report may be repetitive or unduly onerous if they are already performing internal audits, without necessarily adding additional transparency or accountability. Many companies are already performing internal or external audits and making much of the required information available to stakeholders, and so we urge legislators to ensure that the Regulation sets guidelines or criteria for these audit reports, but not necessarily mandate external auditing. The General Data Protection Regulation (GDPR), for example, has shown that internal auditing can be a successful approach to creating awareness of practices within an organisation and supporting accountability for legal standards, without requiring external auditing. There are further practical considerations for example feasibility of auditing in a privacy-compliant way as well as availability of sufficiently qualified auditors capable to audit the large scope of VLOP obligations within the one-year time period envisaged in the DSA.

Article 29: Recommender systems

The obligations in Article 29 to set out main parameters used for their recommender systems in their T&Cs should be careful to not require companies to share any trade secrets or business-confidential information. Requirements on ranking transparency outlined in the Platform-to-Business Regulation overlap considerably with the DSA recommender systems. The Platform-to-Business Regulation states that operators "not be required to disclose algorithms or any information that, with reasonable certainty, would result in the enabling of deception of consumers or consumer harm through the manipulation of search results." It is unclear why the DSA would not provide for the same protections. Consideration should also be given to the context of recommender systems and the risk profiles of those platforms.

Article 30: Additional online advertising transparency obligations

We appreciate the efforts to bring more clarity on online advertising, however we are concerned that these far-reaching requirements would impose significant new burdens on companies without necessarily achieving a particular result. As with recommender systems, consideration of the context of ads and the potential risks should be considered. For example, certain ads, such as political ads or those focused on children, may require additional transparency to understand their reach and content. Further, the value chain in the online advertisement business is quite complex and should be given consideration to account for the different players and their interactions with content and users. Transparency obligations should be placed on the actors in this value chain with the most appropriate ability to access and disclose the required information.

Article 31: Data access and scrutiny

We believe data access requests should relate only to making available, upon request certain, clearly defined types of data collected by VLOPs. However, there need to be clear boundaries as to who can request such data and we believe these should be limited to the Digital Services Coordinator in their Member State of establishment and to the European Commission for the purposes of enforcing this

Regulation. Additional clarification is needed about the circumstances in which this should also be extended to independent academics and researchers whose research projects meet ethical and data security standards. We agree that VLOPs should be equipped with a right for due process and a right to challenge requests received. However, we believe that grounds to refuse requests should be extended to not only include unavailability of data requested or protection of trade secrets but to also include concerns about the requesting institution or academic in particular and the purposes for which it may be used. We are strongly of the view that the details on exact circumstances under which VLOPs have to share data with these groups should not be left to be decided in Delegated Acts as this is an extraordinary power and should instead be specified in the Regulation itself. Lastly, we urge flexibility in the format that data would be transferred in so as not to impose additional disproportionate burden on VLOPs.

Article 34: Voluntary industry standards

We support the Commission's approach to rely on international, voluntary industry standards for notice-and-action systems, trusted flagger notices, APIs and interoperability for online advertisement transparency requirements, and data access. It is important that these be flexible and industry-driven in order to ensure compliance and efficiency. Furthermore, to ensure necessary international compatibility and alignment with a trade- and innovation-facilitative approach to European standardisation, we strongly encourage the Commission to rely on international standards.

Article 35 & 36: Codes of Conduct

Further to the points immediately above, we strongly support reliance on industry-driven, international standards and global best practices in the development of codes of conduct for systemic risks. We appreciate the inclusion of stakeholders in all parts of the ecosystem in the development of such codes. The DSA should include some "guardrails" that define what any code will and will not contain at a high level, for example that these will not mandate practices such as general monitoring. Due process in the development of such codes, including openness, transparency, avoidance of conflict of interest, and well-established, consensus-based voting procedures, ensure that the resulting technical standards will achieve the aim of setting appropriate requirements.

Articles 38-70: Implementation, cooperation, sanctions and enforcement

The Commission proposes to set up a **Digital Services Coordinator** for each Member State and an EU level body called **European Board for Digital Services** composed of a group of Digital Services Coordinators. We encourage the co-legislators to ensure that the enforcement structure does not create multiple accountabilities for a service. We do welcome the amount of detail given on the establishment processes, tasks and voting mechanisms for the European Board of Digital Services. We urge similar clarity on the tasks and objectives of the national Digital Services Coordinators and the European Commission's accountability mechanisms and due process safeguards regarding its proposed enforcement capacity.

However, it is sometimes unclear on what justification certain obligations are based, or what their goal is. For example, equipping the European Commission with powers to conduct **on-site inspections** for VLOPs in specific circumstances seems to miss the goal of obtaining explanations from VLOPs in certain situations. We would welcome clarity on the rationale behind this provision, which should then be incorporated into the text.

We appreciate the importance of responding accurately and promptly to information requests from Digital Services Coordinators, and recognise that in many instances a degree of discussion around the request will be helpful to all parties in clarifying the information that is sought and the forms in which it can be provided. To that end, we would encourage a provision in the Regulation that identifies the benefits of such discussions and allows for good faith requests for clarification.

We would welcome clarifications on the processes and procedural safeguards for joint investigations, and on the methodology to calculate fines, as well as a limitation of the possibility to impose fines only to situations where specific provisions of the Regulation are systematically infringed.

Article 74: Application timeline

We believe that having the Regulation apply from 3 months after its entry into force is not simply very ambitious but clearly unworkable and out of line with the timeframes for implementation of other significant frameworks such as GDPR, the Goods Package or the VAT reforms. The timeframe to allow companies to set up compliance structures should be extended to at least 18 months unless the proposal changes radically toward a more tailored and proportionate approach. We believe that the suggested evaluation cycle of every 5 years is no match for the fast-paced internet economy and should be reduced to every 3 years to assess if the law is still fit for purpose.

* * *