



Access Now's comments on the proposed Digital Services Act (DSA)

Introduction

Access Now welcomes the opportunity to submit comments on the proposed Digital Services Act (DSA) regulatory framework. Access Now has been advocating for a human rights-based and user-centric regulation that will establish clear responsibilities for large online platforms with strong enforcement mechanisms that can hold them to account.

We are pleased to see that the European Commission places the protection of individuals' fundamental rights and freedoms, meaningful transparency, and empowerment of users in the center of a newly proposed regulatory framework. The following comments address the concrete provisions in the proposal that, in our view, can be advanced by the EU co-legislators as recommended in [the Access Now position on the DSA](#) published in 2020.

Our comments focus on the following issues:

1. Measures to establish meaningful transparency
2. Terms and conditions
3. Notice and Action procedure
4. Trusted flaggers
5. Online advertisement
6. Recommender systems
7. Risk assessment and mitigation of risks

Develop measures to establish meaningful transparency

We welcome the fact that the DSA proposal increases the standard of transparency and accountability on how the providers of platforms moderate content, on advertising, and on algorithmic processes. The list of transparency requirements for providers of intermediary services enshrined in Article 13, transparency reporting obligations for providers of online platforms established by Article 23, and additional transparency reporting obligations for very large online platforms (VLOP) under Article 33, are relatively exhaustive and an important positive step towards the systemic regulation of online platforms. The transparency measures

as well as research and evidence-based policy making in content governance are reinforced by Article 31 that provides foundations of data access and scrutiny.

We caution the European Commission and European legislators that highly aggregated statistics about the numbers of complaints and moderation decisions made are not sufficient to draw conclusions about the quality of decisions made by private entities. In order to understand bias in moderation decisions and the algorithms that support them, the inputs and outputs of these systems and their differential social impact need to be provided by VLOP. Analysis of this type will require large-scale access to data on individual moderation decisions as well as deep qualitative analyses of the automated and human processes that platforms deploy internally, including review of false positives and false negatives automated decision making processes generate.

Regulate terms and conditions beyond transparency

Article 12 of the DSA proposal establishes transparency requirements for enforcement of providers' of intermediary services' terms and conditions. While transparency criteria are essential, we note that Article 12 and requirements regarding terms and conditions should be elaborated further.

Terms and conditions remain opaque and thus, their application is unpredictable. Individuals are unable to understand the scope of rules that are meant to regulate their conduct. They are being enforced unevenly and inconsistently across the European Union. At the same time, through the application of their unilaterally decided terms and conditions, a number of very large online platforms have the power to create international standards for restricting free speech online, including by using algorithmic content moderation tools.

Mandate regular notifications to all users about relevant changes of Terms and conditions

All affected parties, current, and new users of all online platforms whose terms and conditions have been amended should be notified of relevant changes, in a user-friendly format. Additionally, users should be able to give meaningful consent, as defined under the General Data Protection Regulation, to these changes, where relevant. Failure to obtain consent should not lead to basic services becoming unavailable.¹

Extend additional transparency requirements

Even if a platform tries to internally ensure consistency in their decision making, users are unaware of these efforts because they are not visible to them. Furthermore, recent research underlined the

¹ Council of Europe, [Recommendation CM/Rec\(2020\)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems](#), 2020.

issue of re-interpretation of terms and conditions by moderators due to their vagueness.² Therefore, online platforms should publish aggregated data on how their content moderation teams are being built up. Such data should include age, nationality, race, gender, and linguistic skills of content moderators as well as whether and how often they receive human rights training. In particular, information about guidelines used by content moderators and what processes exist to support moderators in making consistent decisions should be disclosed to users. All disclosure of data should comply with the General Data Protection Regulation (GDPR).

Provide requirements for procedural fairness in Notice and Action procedure

All notice submitted by any user or entity should not trigger actual knowledge or awareness

According to Article 14(1), any individual or entity may notify providers of hosting services of the presence of specific items of information that the individual or entity considers to be illegal content. The decision whether a notified content is illegal and should be removed or disabled is solely left in the hands of hosting provider services, which is confirmed by recital 40 of the proposal. This, in combination with the fact that any submitted notice can potentially trigger the liability for hosting illegal content, as stipulated in Article 14(3), may intensify online platforms actions to promptly delete a notified content. In this regard, the proposed notice-and-action procedure reaffirms an already existing statu quo, under which online platforms exercise their content governance decisions with no transparency and are not being subjected to any public scrutiny. Furthermore, it is reasonable to expect that the majority of notices will be reviewed and decided upon by the use of automated decision making tools. In this regard, both Article 14 and Article 15 fail to emphasise the importance of human review.

Ensure possibility to submit counter-notification

Counter-notification strengthens the right to fair trial for content providers. It enables them to respond to the evidence and observations that were made by a complainant. This way, content providers are able to present their arguments on equal footing. However, the DSA proposal does not establish such a measure. We note that a notification that is sent to the content provider before any action is taken with regard to the piece of content introduces due process safeguards into the Notice and Action procedure. The purpose of a notification to the content provider is to inform the content provider that a complaint has been made about their content.

² Julia Angwin and Hannes Grassegger, [Facebook's Secret Censorship Rules Protect White Men From Hate Speech But Not Black Children](#), 2017.

However, this notification does not necessarily ensure that the content provider can submit a counter-notification.

Ensure that proposed Notice and Action procedure are tailored to concrete categories of user-generated content

The new legislative framework should provide detailed requirements for Notice and Action procedures because it significantly improves foreseeability and legal certainty for all regulated parties. Access Now has been advocating for a scaled model of responsibility for online platforms and adoption of adequate Notice and action procedures that are tailored to specific categories of user-generated content.³ Different types of illegal online content and activities require different responses specifically tailored to the type of user-generated content in question. We urge lawmakers to address this shortcoming in the DSA proposal.

Specify regulatory measures of trusted flaggers

Trusted flaggers are entities with specific expertise and dedicated structures for detecting and identifying illegal online content. Only independent bodies with specific expertise in content governance with emphasis on disinformation and hate speech should be entitled to become a trusted flagger. The fact that the DSA proposal puts forward the criteria for becoming a trusted flagger is a positive development. The framework provides proper legal safeguards for the impartiality and independence of those trusted flaggers, which should ensure that decisions will be balanced. It should be clarified that such entities should mainly consist of journalistic organisations, public interest groups, and civil society organisations. Law enforcement and other governmental agencies should not be granted a status of a trusted flagger.

Trusted flaggers should lose their status if any conditions for exercising their function are violated. Under no circumstances should the conditions for the institution of trusted flaggers be determined solely by private platforms. We recommend to the European legislator to consider a periodical review of trusted flaggers' status, namely whether the entity still fulfills the conditions set in Article 19(2).

Develop mandatory measures on privacy by design in online advertising

We strongly support the European Commission's effort to enforce more transparency around online advertising in Article 24, including by providing information on whose behalf the advertisement is being displayed and meaningful information about the main parameters to determine the recipient to whom the advertisement is displayed. Article 30 provides additional transparency requirements for online advertisement to be enforced by VLOPs. Yet, considering the current reliance of the ad industry on data harvesting and profiling techniques, transparency

³ Access Now, [Access Now's position on Digital Services Act package: Human Rights-based Framework for Intermediary Liability in Europe](#), 2020.

obligations will not be sufficient to address the impact of industry practices on rights and the economy. In addition to enforcing the GDPR, developing mandatory measures on privacy by design in the ePrivacy reform, we call on the legislator to strengthen rules on advertising in the DSA.

The DSA proposal should establish more robust regulation of online advertising that goes beyond transparency

The European Parliament's Legal Affairs Committee (JURI) adopted a legislative initiative report on the DSA in which it called for regulating targeted advertising, including a phase-out leading to a prohibition. Access Now fully supports calls for stricter regulation of online advertisement. Online advertisement, whether to sell goods, entertainment, or a political idea, has far-reaching impacts on individuals' personal interactions, consumer choices, and participation in democratic debates.

Measures intended to increase transparency can help to better understand the scale of the issues, but these are not enough to prevent and mitigate the abuses. The individual and societal harms created by intrusive targeting and personalisation require a systematic response. It is crucial that the EU puts fundamental rights and freedoms at the centre of how it addresses online tracking and targeting. From privacy violations to content curation, invasive tracking harms our rights to freedom of expression and opinion in tangible ways. In line with the European Data Protection Supervisor (EDPS) opinion on the DSA, we ask the European legislator to consider stricter regulation of online advertisement, including a phase-out leading to a prohibition of profiling based on users' behavioural data and cross-side tracking.

Establish opt-in by default for all platforms using recommender systems

One of the strongest aspects of the draft DSA legal framework is the foundation for meaningful transparency applicable to all service intermediaries, online platforms and VLOP. Article 29 provides another significant step towards human rights centered model of platform governance as it seeks to bring more transparency and increase the explainability of content recommender systems to individuals whose online experience is significantly shaped and impacted by these systems. Article 29 is supported by recital (62), which explains that recommender systems may involve “algorithmically suggesting, ranking and prioritising information, distinguishing through text or other visual representations, or otherwise curating information provided by recipients”.

Content recommendation plays a crucial role in the growth of the majority of online platforms and their business models. Online platforms have an incentive to keep users active and engaged and therefore want to present content that will increase this engagement. The dominant position of VLOPs guarantees them significant regulatory powers over users and their rights as they get to decide how and what users see online: VLOPs become gatekeepers for the exercise of the right to receive information. Their unprecedented access to users' data enables VLOP to deploy recommender systems that “feed on data subjects' profiles and define what

content can be accessed in online platforms, with all the attendant risks.”⁴ Recommender systems are “a key logic governing the flows of information on which we depend.”⁵ Most VLOPs use so-called open recommendation systems, which are partially responsible for contributing to the spread and amplification of potentially harmful user-generated content. To quote a report published by Ranking Digital Rights, “scale matters: the societal impact of a single message or video rises exponentially when a powerful algorithm is driving its distribution.”⁶ Therefore, while transparency is an essential precondition for achieving accountability, the DSA proposal should be more ambitious and provide individuals with empowering tools that will return control over information they receive and impart back to them. We advise the European legislator to extend the scope of Article 29 to all online platforms that curate and moderate user-generated content, and to not limit this measure only to VLOPs.

Article 29 should establish opt-in mechanism to recommender systems by default on all online platforms

Article 29(1) should establish minimum safeguards for users’ default settings to require an “opt-in” to recommender systems to be implemented by all online platforms rather than the current default “opt-out.” We encourage the legislators to clearly specify in the DSA that, in application of the principles of data protection by design and by default guaranteed under Article 25 of the GDPR, online platforms should have personalised content curation systems turned off by default.

Platforms should design “consent” and privacy policies in a way that facilitates informed choice for users and is compliant with data protection laws. Users have to be able to exercise minimal control over recommender systems that can be secured by an “opt-in” mechanism. Making recommender systems available via “opt-in” by default would be a desirable mechanism because even those users who are less aware of how these systems operate will not be treated less favourably.⁷ Access Now position has been recently confirmed by the European Data Protection Supervisor’s Opinion on the DSA: “In accordance with the requirements of data protection by design and by default and data minimisation, the EDPS strongly recommends to modify the requirement to opt-in rather than opt-out, making the option not based on profiling the default one.”⁸

⁴ European Data Protection Supervisor (EDPS), [Opinion 1/2021 on the Proposal for a Digital Services Act](#), 2020.

⁵ Tarleton Gillespie, [Custodians of the internet](#), 2018.

⁶ Nathalie Maréchal, Ellery Roberts Biddle, [It’s Not Just the Content, It’s the Business Model: Democracy’s Online Speech Challenge: A Report from Ranking Digital Rights](#), 2020.

⁷ Access Now, [Access Now’s position on Digital Services Act package: Human Rights Response to the Amplification of Potentially Harmful Legal Content](#), 2020.

⁸ European Data Protection Supervisor (EDPS), [Opinion 1/2021 on the Proposal for a Digital Services Act](#), 2020.

Strengthen Human Rights Impact Assessment requirement in the DSA legislative framework

In Section 4, Chapter III, the DSA proposal establishes a new set of due diligence obligations for VLOP. Article 26 requires that VLOP will conduct risk assessment of significant systemic risks stemming from the functioning and use of their services in the EU. Systemic risks include the dissemination of illegal content, negative effects for the exercise of fundamental rights, particularly the rights to privacy and data protection, freedom of expression, the prohibition of discrimination and the rights of the child and intentional manipulation of their service that is further clarified in point (c). Recital 58 encourages VLOP to cooperate with other service providers, including by initiating or joining existing codes of conduct or other self-regulatory measures.

Do not rely on VLOP's self assessment and self-regulatory measures

One of the main shortcomings of the DSA proposal is the fact that it is solely at the discretion of very large online platforms to identify, analyse, and assess the risk stemming from their services. Under the current proposal, it is exclusively in their and the European Commission's power to assess whether measures to mitigate the systemic risks adopted by VLOP are sufficient or not. Article 27 specifies risk-mitigating measures that VLOP may adopt, including adapting content moderation and content recommender systems and initiating or adjusting cooperation with other platforms through Code of Conducts and crisis protocols. It is important to note that in the context of Code of Practice on disinformation, the European Democracy Action Plan illustrates the future role of self-regulatory Codes and their link to the enforcement of the risk-mitigation measures envisioned by the DSA proposal.

According to the Communication on the European Democracy Action Plan, the DSA should establish “a co-regulatory backstop for the measures which would be included in a revised and strengthened Code of Practice on disinformation.”⁹ Such an approach will significantly strengthen the power of the Code of Practice. However, precisely the self-regulatory nature of the Code is one of the major shortcomings that has been widely criticised by a large number of stakeholders.¹⁰ The Code does not provide sufficient safeguards to ensure the protection of freedom of expression in practice. The 2020 assessment of the Code of Practice underlined the lack of adequate complaint procedures and redress mechanisms for erroneous content demotion or account suspension following a presumed violation of signatories' disinformation policies. Relying on self-reporting from signatories is not sufficient to correctly assess the effectiveness of the Code and its implementation. While the Commission has announced the revision of the Code of Practice, we remain skeptical about the co-regulatory ‘carrot-and-stick’ approach that so far has not delivered on its goals. We therefore urge the legislator to not rely on self-regulatory and self-assessment mechanisms under the DSA.

⁹ European Commission, [Communication on the European Democracy Action Plan](#), 2020.

¹⁰ Access Now, Civil Liberties Union for Europe, European Digital Rights, [Informing the Disinformation Debate](#), 2018.

Include a requirement for a mandatory Human Rights Impact Assessment

Mandatory human rights impact assessments (HRIA) should be the primary mechanism for identifying and assessing systemic risks stemming from VLOP's functioning and use of their services. Currently, the DSA only requires for HRIA once a risk has been identified which would greatly limit their scope.

We welcome that Article 26(b) refers to systemic risks for the exercise of fundamental rights as enshrined in the Charter. Nevertheless, all online platforms that use content moderation systems, content recommender systems, and systems for selecting and displaying advertisements should be obliged to conduct mandatory HRIA and use this rights-based assessment to identify risks. This obligation should not be limited to VLOP only. The summary or a redacted version of the HRIA should be made publicly available and accessible and all information need to be communicated to all relevant stakeholders, including regulators and enforcement bodies, in a continuous manner, for the purposes of independent audits. In addition, and based on Access Now's expertise in the field of Artificial Intelligence (AI) and data protection, we strongly argue that the assessment of all operations of VLOP, including their use of automated decision making (ADM) or 'AI' systems, should be conducted on the basis of an analysis on human rights impact and not be limited to a risk mitigation exercise. The burden of proof should be on VLOP to demonstrate that their services as whole and their individual products and technical tools do not violate human rights via a mandatory HRIA. The HRIA should determine the level of risk posed to human rights, and thereby determine which safeguards must be assigned to the specific impacts established in the process. The mitigation of risks can only come as a second, complementary step once the full range of impact on human rights has been determined by the HRIA.¹¹

Risks identified and measures taken to avoid or mitigate those risks must be documented, and updated throughout the lifecycle of systems and operations deployed by VLOP that enable functioning of their service. We caution against any regulatory mode that is based on a rigid binary distinction between low and high systemic risks. As discussed within the context of the GDPR, a significant loophole was left open by allowing the data controller to determine alone whether a system poses a high risk and whether a data protection impact assessment is needed. This leaves open a scenario in which risks could in fact be downplayed, leading to a reduction in user safeguards.

Additionally, during the GDPR negotiations, the EU data protection authorities further recalled that "rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved". We must therefore avoid a situation in which responsible VLOP can shirk their responsibilities by ignoring rights. The legislators should clarify that a risk assessment should be publicly available and can only complement obligations to respect fundamental rights, and not replace it.

¹¹ Access Now, [Access Now's submission to the Consultation on the "White Paper on Artificial Intelligence - a European approach to excellence and trust"](#), 2020.

Finally, the outcome of mandatory HRIA can significantly vary depending on who conducts them. We propose to the European Parliament and the Council of the EU to amend the DSA proposal by introducing a contestability mechanism for independent stakeholders, such as human rights organisations and equality bodies, that will be able to challenge the outcome of the HRIA if there is a sufficient evidence that platforms' operations have negative effects for the exercise of the fundamental rights. Especially, Equality bodies have a vital role in addressing any adverse effect of ADM and AI systems that they may have on equality and non-discrimination of underrepresented groups. It is crucial for the EU and its Member States to enable them to play this role by providing them with adequate and meaningful powers and secure and sufficient resources. The European Network of Equality Bodies (EQUINET) sets forward the list of recommendations for strengthening their position in this field.¹² At the minimum, equality bodies should be able to undertake strategic litigation to challenge discriminatory outcomes of automated measures, to have a dedicated team of staff members conducting HRIA and to work towards enhancing transparency in ADMs.

Conclusion

We thank you for the opportunity to provide comments to the proposed Digital Services Act. For more information, including recommendations on oversights, we refer to our full position on the DSA.¹³

We remain available for any questions you may have and we look forward to engaging with the European Parliament and Council of the European Union in further strengthening the proposed Digital Services Act with the view of delivering a robust framework for the protection of users' fundamental rights and freedoms.

For more information, please contact:

Eliska Pirkova

Europe Policy Analyst

eliska@accessnow.org

¹² EQUINET, [Regulating for an equal AI: A new role for equality bodies - Meeting the new challenges to equality and non-discrimination from increased digitisation and the use of Artificial Intelligence](#), 2020.

¹³ Access Now, [Access Now's position on the Digital Services Act Package](#), 2020.