Civil Society Statement of Key Principles
Committee on Civil Liberties, Justice and Home Affairs (LIBE)
Report on the draft Digital Services Act

Brussels, June 8th 2021

We are a coalition of leading human rights organisations working on EU digital law and policy. We issue this statement in advance of the preparation of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) Opinion on the Digital Services Act (DSA), and further to the draft LIBE Opinion on the DSA issued last month.

We welcome the DSA's many positive provisions that could significantly improve the transparency and accountability of internet intermediaries, and ensure a safer, more vibrant online civic space. For example, the increased focus on **fundamental rights** throughout the draft is a welcome approach. The DSA also maintains the cornerstones of rights protection from the E-commerce Directive, namely **conditional immunity from liability** for hosting providers and **the prohibition on general monitoring.** We additionally welcome the **wide-ranging transparency obligations** that the DSA introduces, including transparency reporting in relation to how user complaints are handled, increased transparency over recommender systems and algorithms, and transparency obligations on intermediaries in relation to their terms of services and statements of reasons for decisions.

There are, however, a number of important improvements that need to be made to the current draft in order to ensure that fundamental rights and democractic principles are upheld. We welcome that the draft LIBE Opinion has taken many of these considerations on board, and would urge all members to vote in support of these welcome changes.

1. **Uphold the prohibition on general monitoring in practice**

The DSA explicitly states that "Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or active fact-finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content." (Recital. 28) The DSA also establishes that intermediaries do not jeopardise their safe harbor protections solely by "carrying

out voluntary own-initiative investigations [. . .] aimed at detecting, identifying and removing or disabling access to illegal content" (Article 6). Thus, while the DSA does not directly require intermediaries to employ proactive measures, it does seek to eliminate disincentives to do so. Moreover, Article 35 gives the European Commission and the Board broad powers to draw up "Codes of Conduct" to "contribute to the proper application of" the DSA; Recital 28 may indicate that proactive measures are not a viable component of such Codes, but this is far from certain.

Furthermore, Art. 21 would create a new obligation for platforms to "notify of suspicious criminal offences." This is not an appropriate role for a private company. It risks undermining individuals' privacy in their digital communications, the right of presumption of innocence and EU criminal law's own protections with regard to notice that an individual is a suspect. Companies will face every incentive to over-report on their users, rather than risk liability for themselves, leading to substantial amounts of useless and distracting information for law enforcement while severely threatening the fundamental rights of internet users. Such a policy is likely to disproportionately affect already marginalised and vulnerable groups and individuals who already face stigma and discrimination in society.

We welcome the deletion of Art. 35 (1) in the draft LIBE Opinion, which recognises the threat to fundamental rights that inclusion of the Codes of Conduct in the Regulation would have. Whilst we welcome the narrowing of the scope of Art. 21 (or the deletion of Art. 21 entirely), the new text remains problematic and would be better to be deleted.

2. Protect online expression of users

It is well established under international human rights law that overly broad liability regimes for online platforms pose a serious threat to freedom of expression. Whilst it is important that intermediaries be subject to a clear procedure when responding to notices, they should not become liable for the content upon notices of *allegedly* illegal content from average users, law enforcement, or other non-judicial actors. In Art. 14, the current draft DSA exposes intermediaries to the threat of legal liability whenever they receive notice from any user claiming that a piece of content is illegal. Such a provision would inevitably lead to intermediaries erring on the side of caution and over-removing content to avoid liability. This approach also betrays the objective of the public interest by placing the decisions on legality of speech into the hands of private companies.

International and European human rights law is clear that decisions on the legality of speech are the sole purview of the courts. The draft DSA, however, conflates intermediaries' terms of service (TOS) with what the State has designated as illegal speech. It creates a structure whereby companies decide whether a post constitutes illegal content and/or violates their TOS through their internal complaints handling system (Art. 17 (3)). Although appeals can be made through the out-of-court dispute settlement process (Art. 18), this system does not meet the standard of a tribunal under the EU Charter of Fundamental Rights given its lack of

independence and impartiality.[1] This means that the overall impact is placing questions on the legality of speech in the hands of the companies or nonjudicial state authorities. Judicial redress should always be available in practice to all affected parties, regardless of which notice and action procedures were triggered.

We support the draft LIBE Opinon's approach that introduces amendments to protect freedom of expression and media freedom through ensuring that the decision on the legality of content should rest with the independent judiciary, not with administrative authorities. Further clarity should also be introduced to underpin that users always have recourse to a Court.

3. Phase out advertising based on pervasive tracking

Disinformation campaigns are frequently designed deliberately as a tool to promote racist and misogynistic content. Minorities and human rights defenders are frequent targets of online hate and disinformation. This is nothing new, but the extent of these attacks in Europe is novel, as is the brutal efficacy with which they can be executed on online platforms by profiling users' personal data and exploiting their prejudices. The adverse effects of this model have also been demonstrated in the context of election interference and microtargeting.

More generally, the surveillance-based business model is inherently incompatible with the right to privacy, and poses a threat to a range of other rights including freedom of opinion and expression, freedom of thought, and the right to equality and nondiscrimination. This is why we concur with the opinion of the European Data Protection Supervisor that recommender systems should by default not be based on profiling within the meaning of Art. 4(4) of the GDPR, and that advertising based on pervasive tracking needs to be phased out.

We therefore welcome the draft LIBE Opinion's proposal to phase out behavioral advertising.

4. Focus due diligence obligations on companies, not users

The DSA has adopted a "good samaritan" provision for the first time in Art. 6. This is to be welcomed, though this provision is limited to when intermediaries carry out voluntary measures on their own initiative or when they seek to comply with EU law. It is not clear, however, given the broad scope of due diligence obligations combined with the current "notice equals knowledge" notice-and-action framework, to what extent intermediaries could lose immunity from liability for their handling of user-generated content.

The inclusion of human rights impact assessments could be a welcome addition to the DSA. However, the current vagueness in the Draft's risk assessment obligations for very large online

[1] Art. 47, the EU Charter of Fundamental Rights, the right to an effective remedy and to a fair trial.

platforms (VLOPs) (Art. 26), including the obligation to prevent the "dissemination of illegal content," creates a conflict with the earlier provision prohibiting general monitoring and also with Art. 26(1)(b) on protecting fundamental rights (e.g., in the sense that excessive removal of content would violate free speech rights). Furthermore, Recital 25 states that platforms must act in a good-faith and diligent manner with regard to content moderation. However there is little clarification about what that constitutes.

The UN Guiding Principles on Business and Human Rights calls on companies to conduct due diligence that identifies, addresses, and accounts for actual and potential human rights impacts of their activities. The challenge with the current draft of the DSA is that it asks for due diligence in enforcing, e.g., EU codes of conduct and other vague provisions on the removal of "illegal" speech. Complying with these guidelines and provisions is likely to in fact lead to violations of free expression and privacy rights due to the incentives that have been created to monitor and censor. A system, therefore, that assessed the overall human rights impact of the DSA including companies' implementation could be more effective in catching and mitigating against actual human rights violations.

Due diligence obligations should be on companies with regard to the human rights violations linked to their products and services, not about their obligation to surveil user content.

While we agree with the concerns related to fundamental rights that the LIBE rapporteur has raised in his justification of the deletion of Art. 26, we feel that there should still be a due diligence regime maintained, but that it would be more appropriate for such a system to focus directly on the human rights impact of products and services of intermediaries and not on the removal of user-generated content.

5. **Consider the global impact on civic space**

The DSA's extension of personal liability to the "legal representatives" required to be designated under Article 11 is unnecessary and will further incentivise mass surveillance and policing of users. It also sets a troubling precedent as non-democratic governments insert "hostage provisions" in their content regulations in order to increase their leverage over intermediaries. Too often this is used to pressure intermediaries into complying with requests to clamp down on the content of human rights defenders and journalists, or as a way to threaten intermediaries who take legitimate steps to moderate the abusive speech of politicians. Furthermore, such a requirement is disproportionate for small providers, in particular providers based outside the European Union, which may stop offering services to the EU if facing the hassle and costs to appoint legal representatives. This also undermines users' access to information rights. If this provision is retained, very small providers that provide services in or to the EU should be excluded from the requirement to appoint a legal representative.

Art. 19 requires that providers create the ability for trusted flaggers to submit notifications about allegedly illegal content, and requires that providers prioritise these notifications. Digital Service

Coordinators may designate trusted flagger organisations based in the same Member State. A trusted flagger can also be a law enforcement authority. This poses a serious problem in two ways. Firstly, law enforcement authorities should always be subject to strict checks and balances, including judicial orders when wishing to remove content or gain access to users. Mandating them by law here as trusted flaggers would circumvent essential rule of law safeguards. Secondly, particularly but not exclusively in countries where the rule of law is under threat, state-selected and legally mandated trusted flaggers could have a serious negative impact on human rights defenders, journalists, or other dissenting voices.

We would call on LIBE members to make an amendment to ensure the deletion of Art. 11. We do not feel that the proposed amendments to Art. 19 on trusted flaggers go far enough, because the amendments do not respond to the concerns as outlined above.

Signatories:

Access Now
ARTICLE 19
Centre for Democracy & Technology, Europe
Electronic Frontier Foundation