

Dear Members of the European Parliament,

We, the undersigned civil society organisations, are writing to share our concerns about recent suggestions to the proposed Digital Services Act that are currently being negotiated in the European Parliament. We highlight below human rights-based concepts that must be respected, and proposals currently debated in the European Parliament that could abandon core tenets that made the internet free and jeopardize the goal of creating a human rights-centric model of platform governance.

The proposed Digital Services Act (DSA) offers an unparalleled opportunity to reinvigorate transparency and openness, and return agency and control over information to Internet users. If done right, the DSA can address some of today's most pressing challenges and help better protect fundamental rights online. However, if done wrong, it can endanger freedom of expression and have a devastating effect for vulnerable communities.

We welcome the significant efforts by leading MEPs in the responsible European Parliament committees to shape new rules aimed at modernizing the e-Commerce Directive. Procedural justice elements, more transparency online, and a human-rights based approach for regulating intermediary liability are important additions to current internet rules. However, we are very concerned about certain proposals we believe could easily undermine pillars of the e-Commerce Directive that are crucial in a free and democratic society. Free speech online, protection of marginalized groups, and respect for users' private communication are key principles that should not be up for negotiation.

Knowledge-based Intermediary Liability System in Danger

To safeguard the protection of fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (EU Charter), the proposed Digital Services Act must follow the e-Commerce Directive and provide intermediary liability exemptions and prohibit mandated general monitoring of user-generated content by internet intermediaries.

The suggestion to prevent intermediaries that “optimise, classify, organise or otherwise promote the online content” from benefiting from liability exemptions, currently proposed in the JURI Draft Report, fails to acknowledge that content moderation and content curation are basic functions of social media platforms. The question should not be whether online platforms are allowed to moderate and curate user-generated content, but how they exercise such operations and what due diligence safeguards are in place to protect fundamental rights and ensure fairness and consistency. Any other interpretation contradicts [EU Court of Justice case law](#), which recognizes that intermediaries are exempt from liability unless their active role gives rise to “actual knowledge” (what platform providers really know) or control over illegal content and platforms fail to remove it.

Another equally problematic proposal in the JURI Draft Report suggests that liability exemptions in the proposed DSA should not be available to intermediary service providers that do not comply with the due diligence obligations as defined in Section 4, Chapter III. Non-compliance with due diligence safeguards should never result in losing liability protection, as this would intensify over-compliance and thus over-removals of legitimate content at large scale. The main purpose of due-diligence safeguards is to bring systems and operations deployed by private platforms under public scrutiny and to empower

individuals in the online ecosystem. Using them as the tool to force platforms to comply with regulatory demands under the threat of liability goes directly against the essence of these novel provisions and the intention of the drafters.

Bottom Line: The Digital Services Act should uphold the existing conditional intermediary liability model in the EU. Any modifications that result in short-sighted content removals of legitimate speech or which otherwise do not comply with fundamental rights protections under the EU Charter and the jurisprudence of the Court of Justice should be rejected.

Don't Interfere with Private Communication

Protecting the privacy of users and their personal data is a fundamental right laid down in the EU Charter and could be undermined if lawmakers were to force companies to analyse and indiscriminately monitor users' communication. We are convinced that such regulations have no place in the DSA. Notice and action systems or the DSA's rules on transparency and redress are not apt to deal with private messaging services like WhatsApp or Signal. Users of such services rely on end-to-end encryption and have enhanced security and privacy expectations.

Specific rules for messaging services should be addressed in specific legal instruments, such as the ePrivacy Regulation, and not rushed into the DSA, which, for good reason, intended to leave interpersonal communication services out of its scope. The suggestion by some MEPs to differentiate between private and non-private and commercial and non-commercial messaging services comes without any clear definitions and fails to consider the dynamic nature of chat groups and the multiplicity of services on which users rely in their everyday interactions. We also recommend opposing language that incentivises the use of intrusive monitoring of user communications. A duty of care to prevent the re-upload of content can only be met using upload filters and will effectively put an end to private communication. Human review or other ex-post safeguards cannot compensate for such intrusive measures.

Bottom Line: The Digital Services Act should honor users' expectation of privacy and protect their right to communicate free of monitoring and censorship.

Trusting Trusted Flaggers and Prioritization of Content

Trusted flaggers are entities with specific expertise and dedicated structures for detecting and identifying illegal online content. They should act independently from online platforms, commercial entities, and law enforcement agencies and have the collective interests of the public and the protection of fundamental rights in mind. The DSA proposal setting out criteria for becoming a trusted flagger falls short of these safeguards. It allows governmental and law enforcement agencies, which often only follow efficiency objectives, to be awarded the status of trusted flaggers and obligates platforms to treat their notices with priority, opening the door to potential notice, action, and human rights misuse.

A proposal by the IMCO draft report could make the situation for users even worse—it says public authorities should be treated as trustworthy sources for recommender systems and ranked higher. This faulty approach is mirrored by special, must-carry protections for public

interest accounts, such as those held by politicians, which would lead to a two-class society online where powerful account holders receive special advantages not available to ordinary users.

Bottom Line: Platforms should not be forced to apply one set of rules to ordinary users and a more permissive set of rules to influencer accounts and politicians. First-class treatment for sources and notifications of non-independent authorities or commercial entities should be rejected.

Unduly Short and Strict Time Frames for Content Removals and Proactive Measures

We urge European legislators to refrain from imposing short and unreasonable time frames for content removal, as this would increase the over-removal of legitimate speech from platforms. The e-Commerce Directive acknowledges the need for flexibility and for upholding freedom of expression and thus abstains from introducing any fixed period to act after a service provider has become aware or obtained knowledge of illegal activity.

Proposals by the IMCO and JURI Draft Reports suggest removing content within deadlines as short as 30-minutes or 24 hours. If this were to become law, it would compel platforms to deploy automated filtering technologies at scale, which runs afoul of the prohibition against general online content monitoring and violates the rights to freedom of expression and privacy. Strict and short deadlines for content removals cannot be reconciled with the EU's Charter of Fundamental Rights, while recent national proposals that follow the same approach are under increased constitutional scrutiny. For example, short deadlines for removing online hate speech and other types of illegal content have recently been declared [unconstitutional](#) by the Constitutional Council of France due to their negative impact on users' right to freedom of expression.

Similarly, [the Council of Europe Recommendation on the roles and responsibilities of internet intermediaries](#) establishes that state authorities "should not directly or indirectly impose a general obligation on platforms to monitor content which they merely give access to, or which they transmit or store, be it by automated means or not." In his 2018 report on the promotion and protection of the right to freedom of opinion and expression, the UN Special Rapporteur clarified that states should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, as it would be both inconsistent with the right to privacy and likely to amount to pre-publication censorship.

Bottom Line: Inflexible and short deadlines for content removals will lead to upload filters and cannot be reconciled with fundamental rights of users.

Sincerely yours,

Access Now, International

Association for Technology and Internet, Romania

Bits of Freedom, Netherlands

Center for Democracy and Technology, Europe
Committee to Protect Journalists, International
Digitale Gesellschaft, Germany
European Digital Rights (EDRi), Europe
Electronic Frontier Foundation, International
Electronic Frontier Norway, Norway
Epicenter.works, Austria
IT-Pol, Denmark
Panoptikon Foundation, Poland
Privacy International, international
Xnet, Spain