BRIEFING: Priorities for the Digital Services Act Trilogues

The Digital Services Act (DSA) is a crucial and welcome opportunity to hold online platforms to account and ensure a safer and more transparent online environment for all. EU negotiators must ensure that the DSA has the protection of citizens' fundamental rights and democracy at its core, establishing meaningful long-term accountability and scrutiny of online platforms. Key outstanding issues must be resolved in the trilogues, including EU-level enforcement, due diligence requirements, data scrutiny and tackling systemic risks related to tracking-based advertising.

As the DSA negotiations progress, we therefore urge you to prioritise the following issues:

➔ **A strong EU-level enforcement regime for VLOPs** (Art 50)

We commend the Council for its support for an EU-level enforcement structure, as confirmed in the General Approach, and recommend giving **enforcement powers to an independent unit inside the European Commission to oversee VLOPs**. Matched with adequate resources, we believe independent EU-level enforcement powers offer the best opportunity for ensuring deep and consistent checks of VLOP's compliance with due diligence measures from the outset. We urge you to prioritise this in the negotiations, avoiding the pitfalls of fragmentation and delay that has plagued other EU legislation such as the GDPR.

➔ **Tackling the most egregious forms of tracking-based advertising** (Art 24)

The European Parliament's DSA position secures important new safeguards against some of the most egregious and invasive forms of profiling for tracking-based advertising: **minors and sensitive data** - including sexual orientation, health data, or religious and political beliefs**.** EU policymakers must urgently guarantee this protection for citizens. This type of data should not be used for advertising purposes, given the inherent systemic risks posed. Recent polling from Global Witness and Amnesty Tech in France and Germany has shown that not only citizens are deeply uncomfortable with their sensitive data being used for advertising, but SMEs are also wary, believing their own customers would disapprove and wanting to see more regulation.

➔ **An end to manipulative practices and fair access** (Art 13a & 24)

If the DSA is meant to truly empower users and protect fundamental rights, platforms must be prevented from using manipulative design techniques, or "dark patterns", to coerce users' consent and decisions. The Parliament's addition of Article 13a on "Online interface design and organisation" is an essential development for safeguarding users' rights and protect them from unfair consumer practices. This must include the ability for users to indicate their opt out **preference in the browser** via a legally binding "do not track" signal, sparing them from continuous consent banners. **Refusing consent should be just as easy** as giving it and users who reject tracking should still have **alternative access** options which are fair and reasonable (Art 13a 1; Art 24 1a).

➔ **Ensuring meaningful third-party scrutiny of VLOPs** (Art 31)

While we welcome the DSA's ambition to mandate data scrutiny of VLOPs by third parties in relation to their systemic risks, we are concerned this crucial oversight measure will be severely weakened if it is limited to academics and if platforms are able to invoke a broad **"trade secrets" exemption**. Given the crucial role **civil society organisations** play in holding platforms to account and exposing rights breaches and other harms, access should be extended to them - provided their proposals adhere to the highest ethical and methodological standards and they are able to secure any personal data they receive. Currently, scrutiny is severely hampered by the lack of data available as well as a hostile approach from key platforms. This includes Facebook's intimidation of AlgorithmWatch to shut down its Instagram Monitoring Project by weaponizing the company's terms of service. We therefore strongly urge you to support the Parliament's position to widen access to include *"vetted not-for-profit bodies, organisations or associations"* and remove the trade secrets exemption.

➔ **Widening risk assessment to cover all rights and social harms** (Art 26 and 27)

We urge you to support the Parliament's position on risk assessment and clarify the text to ensure that it expands risk assessment to consider **all fundamental rights** as set out in the EU Charter of Fundamental Rights, while maintaining a focus on social harms such as disinformation. This expansion is essential to ensure risk assessment is comprehensive and sufficiently addresses all systemic risks - current and future. A crucial addition from the Parliament's position is to ensure assessments of risks posed by algorithms, activities, and business-model choices, **before** new products are deployed as well as explicit focus on VLOPs' **business model choices** and inclusion of risks stemming from "**algorithmic systems**". Finally, the DSA should require that **civil society organisations** be consulted as part of VLOPs' risk assessment and when designing risk mitigation measures, as the Parliament's position underlines (Art 26 2a; Art 27 1a). This is essential as a check on potential negative effects of mitigation measures on citizens or minorities, such as discriminatory moderation or over-removal of content.

➔ **Empowering users to seek redress** (Art 17)

We commend the Council for its position regarding the **internal complaint handling system**, empowering users to seek redress against wrongful actions and inactions by the platforms. As the General Approach makes clear, the system must be broadened so it covers all cases, including where users want to act **when a platform has not removed or disabled access** to a piece of content. Failing to broaden the application of this Article would further harm victims of hate speech and vulnerable communities, who would be left powerless. We therefore strongly urge you to follow Council's position (by including "*whether or not*" in Art.17 (1)) and provide redress through internal complaint handling mechanisms to all users.

This briefing paper has been compiled by Algorithm Watch, Alliance 4 Europe, Amnesty International, Association for Technology and Internet (ApTI), Avaaz, Defend Democracy, Global Witness, Hate Aid, Je Suis Là, Panoptykon Foundation, SumOfUs, Signals Network, Vrijschrift.