PANOPTYKON FOUNDATION

22 September 2021

Dear IMCO Committee Members,

As you debate the European Parliament's position on the Digital Services Act, the undersigned organisations urge you to ensure effective oversight of the algorithms used by large online platforms that shape our experience of the world. We need accountability for the individual and societal effects of these technologies, so that they have a positive impact on our lives.

In this letter we explain the core problems that the power over algorithms pose and outline key areas where we believe the Commission's DSA proposal requires amendment.

We strongly recommend that you:

1. **Require the disclosure of all key information about algorithms to users.**
2. **Extend access to data necessary to monitor the use of algorithms to civil society organizations and journalists.**
3. **Submit platforms' risk assessments to independent audits.**
4. **Introduce default protection for users against intrusive use of their personal data and deceptive interfaces.**
5. **Increase user control over the operation of recommender systems.**
6. **Empower users to choose their preferred third-party recommender systems independent of the options offered by the platform.**

The Black Box Behind the Screen

The internet is dominated by platforms which personalise our exposure to content through algorithmic selection. Public debate and life opportunities are significantly shaped by their decisions about what to show, to whom, and when.[1] With great power should come great accountability, but instead **the logic behind their algorithmic choices remains opaque.** The business model of most platforms, **surveillance-based advertising,** has commercial priorities that collide with the interests of the individual and the public good.[2] The terms of the resulting tradeoff are at stake in this regulatory reform.

Risks of Inference-Based Targeting and Lack of User Control

Facebook, Youtube, and other platforms that rely on surveillance-based advertising engineer systems to maximize user time-on-platform and select users who will respond in the manner specified by the advertiser.[3] But the push for performance can result in unwelcome intrusions. This happens when **platforms infer highly sensitive information about their users based on machine learning models**, which the users have not provided themselves. The user may not want to disclose their sexuality, religion, or anxieties, but the data about their interactions with the service can generate predictions about these traits nevertheless. These attributes are mostly

[1] For example, recommendations drive 70% of views on Youtube and 95% on Tiktok.
[2] More than 80% of Alphabet's revenue and nearly 98% of Facebook's comes from advertising.
[3] See: https://www.newamerica.org/oti/reports/special-delivery/

undisclosed and not modifiable in the user's profile, but rather exist as latent knowledge, used to enhance predictions about what a user is most likely to click on and hence make them spend more time on the platform. **But these inferences, whether accurate or not, can have negative ramifications for users.**

Discriminatory Effects and Amplification of the Awful

Ad delivery algorithms, which select audiences from larger sets of eligible viewers, have been shown to discriminate against people based on gender, race, or age with respect to their access to job or housing offers.[4] This may result from the use of historical data which reflects societal inequities, proxies for protected characteristics (e.g. the time spent on the platform might be a proxy for age or employment status), market-based factors[5], or because members of the group have previously been more responsive. **Advertisers may not intend to discriminate against protected groups but the algorithmic fixation on campaign targets can have that effect.**[6] Although the outcome is sometimes unintended, the discriminatory impact is significant.

Recommender systems have similar flaws. The search to match users with 'engaging' material can result in the amplification of content which provokes responses because it is inflammatory, unreliable, or sensationalist, while secrecy shields platforms from criticism for these choices and users are not empowered to engage with these platforms using different recommendation schemes.[7] It can also promote material to users which endangers their physical or mental health.[8] Whenever the press describes the stories of the affected individuals, platforms try to mitigate on a per-case basis, but the cycle inevitably repeats. These companies then provide assurances without giving any visibility into the algorithm or how it has been modified, nor do they allow access to system-level data to quantify the scale of the damage and hold platforms to account.[9] **Think of an oil spill where you don't know why the accident happened or the size of the slick.**

Services such as Facebook require users to abdicate control over their data as a condition of access. Those unhappy with their privacy practices or recommendations are currently cornered. Leaving is hard and user controls are ineffective, especially when it comes to inference-driven targeting.

Essential Areas for Amendment

The Commission's DSA proposal does not adequately address the information deficit around algorithms used to curate and personalise content. Nor does it protect users from discriminatory effects, or create the conditions for real competition and user choice in the market for recommender systems. We urge you to make the following amendments:

---

[4] See for example: https://algorithmwatch.org/en/automated-discrimination-facebook-google/
[5] Women are more sought after as an audience and thus more expensive. See: https://doi.org/10.1287/mnsc.2018.3093
[6] Facebook banned discriminatory targeting of housing and employment ads, but their delivery algorithm skews outcomes anyway. See: https://dl.acm.org/doi/abs/10.1145/3359301
[7] Facebook's algorithm rewards outrage but the company resists fixes because they would lead users to interact with the platform less: https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215?mod=article_inline
[8] Searches for dieting advice can quickly lead to suggestions for pro-anorexia videos. For user testimonies about rabbit holes, https://foundation.mozilla.org/en/campaigns/youtube-regrets/
[9] It is indicative that the investigation of potential voter manipulation on Facebook during the US presidential elections in 2016 was carried out by the company rather than an external auditor.

1. Extend the Transparency Requirements

Algorithmic risk requires careful oversight, but this is impeded by lack of information about algorithm design. Article 24 (advertising) and Article 29 (recommender systems) require limited disclosures by entities using such systems and - in the case of advertising - focus only on advertisers' targeting attributes, and not the platform's choices. **These must be extended to cover all key information about the algorithm**: the specific *goals* for which it is optimised (e.g. watch time on Youtube), the *key parameters* that the system relies on, their *influence* on what content is displayed, and how *data on user behaviour* affects recommendations and ad targeting.

2. Extend Access to Data to Civil Society and Journalists

Article 31 provides for access to system-level data by regulators and vetted academic researchers to audit algorithmic operations and effects. This provision should be extended to investigative journalists and watchdog groups, who have already proved crucial in uncovering harmful consequences of algorithms and will continue to be key players in scrutinizing the impact of these systems. Data access must be compliant with the GDPR and include safeguards to minimize any privacy risks and to prevent improper use of the data.

3. Subject Self-Assessments of Risk to Independent Audits

Under Article 26, VLOPs should be required to assess potential risks to **all** fundamental rights and the societal effects of their systems. **Self-assessments will be worthless unless audited by independent entities, whether public or vetted by the regulator.** Supervisory authorities should develop guidelines for what these assessments and audits should look like.

4. Protect Users By Default from Intrusive Inferences and Dark Patterns

Users should be shielded from coercive terms by a new provision **mandating that the default mode of access to platform services should exclude use of personal data for both recommendations and advertising.** In addition, consent settings over data use should be controllable via a user-friendly interface independent of the platform.[10] The use of visually deceptive interfaces to manipulate or impair user choice, 'dark patterns', should be banned.[11]

5. Enable Users To Modify Recommendation Systems

Article 29 currently requires an option to choose a recommender system that is not based on profiling. As stated above, this opt-out should be an opt-in by default. Other than that, platforms can offer their existing algorithms on an all or nothing basis. But it should be a requirement, and not a voluntary option, to enable user modification of the algorithms' goals and parameters.

6. Empower Users Through Ecosystem Innovation

Ultimately, algorithmic performance should be a terrain where entities, commercial and non-profit, compete to empower users. We propose a change to Article 29 which would give **users the choice to use their preferred third-party recommender system, for which the platform would have to guarantee interoperability**.[12]

---

[10] See for example the Do Not Track feature common in browsers.
[11] The California Privacy Rights Act has banned dark patterns.
[12] See one of the first examples of how a third-party recommender system could work: http://youchoose.ai

This would mean unbundling the hosting and curation functions currently centralised in the platforms. In the telecommunications sector, rival services compete on the same infrastructure - in a platform context the incumbent would continue to host the content, but third parties could offer services built on top.[13] This would also exert pressure on platform operators to be responsive to criticism.

Finally, even the most perfect regulatory scheme is meaningless without a proper enforcement structure, it is vital that supervisory bodies have the necessary expertise and are bound by procedural rules which ensure timely intervention and effective corrective measures.

The DSA is a unique opportunity to craft innovative solutions for a digital world which has lost its innocence but where the opportunities for citizens are still great. We urge you to adopt these proposals which can ensure that Europe's digital future is built on fundamental rights, consumer protection, and innovation that benefits society.

Yours sincerely,

Access Now
Algorithm Watch
Alternatif Bilisim (AIA, Turkey)
Amnesty International
Article 19
Association for Technology and Internet (ApTI)
Átlátszó Erdély
Balkan Investigative Reporting Network (BIRN)
Bits of Freedom
Civil Liberties Union for Europe (Liberties)
D3 - Defesa dos Direitos Digitais
Digitalcourage
Digitale Gesellschaft
Državljan D / Citizen D
Electronic Frontier Foundation (EFF)
Electronic Frontier Norway (EFN)
European Center for Not-for-Profit Law (ECNL)
European Digital Rights (EDRi)
European Partnership for Democracy (EPD[14]
Global Forum for Media Development (GFMD)
Global Witness
Gong
Helsinki Foundation for Human Rights
Homo Digitalis
Irish Council for Civil Liberties
Italian Coalition for Civil Liberties and Rights (CILD)
IT-Pol Denmark
OpenMedia
Panoptykon Foundation
Privacy International
Ranking Digital Rights
Stiftung Neue Verantwortung (SNV)
Tracking Exposed
Xnet

[13] Third-party providers would have to comply with the GDPR and other regulatory safeguards.
[14] On behalf of 18 member organisations: Agence Française de Développement Médias (CFI) | Article19 | Danish Institute for Parties and Democracy (DIPD) | Demo Finland | elbarlament | European Association for Local Democracy (ALDA) | European Centre for Electoral Support (ECES) | Netherlands Helsinki Committee (NHC) | Netherlands Institute for Multiparty Democracy (NIMD) | OneWorld | The Oslo Center | People in Need (PIN) | The Universidade Católica Portuguesa | Westminster Foundation for Democracy (WFD) | World Leadership Alliance - Club de Madrid | Election Watch EU | Democracy Reporting International | EDGE (Experts in Democracy, Governance and Elections).