

/ Position by AlgorithmWatch

## **The DSA proposal is a good start. Now policymakers must ensure that it has teeth.**

December 2020

*Authors: Mackenzie Nelson & Friederike Reinhold*

**Yesterday, the European Commission unveiled two of the most anticipated components of its digital agenda: The Digital Services Act (DSA) and the Digital Markets Act (DMA). The [DSA proposal](#) introduces new rules on how online marketplaces and content hosting platforms deal with illegal content, including special transparency and auditing obligations for very large platforms with more than 45 million monthly active users in the EU, a threshold surpassed by several services including Facebook, YouTube, Twitter and TikTok. While the DMA will be an important and contested piece of legislation, especially with regard to competition questions, this response will focus on the DSA.**

[Speaking at our October 2020 policy dialogue](#), Executive Vice President (EVP) Margarethe Vestager stressed that the ultimate goal of the DSA/DMA packages is to translate Europe's "analogue" values system into the online realm, and ensure that decisions that affect the future of our democracy aren't confined to the "secrecy of a few corporate boardrooms." Upon our initial review, we are optimistic that the DSA is a step in the right direction, but key dimensions will require more attention. As the draft makes its way through the long legislative process ahead (the European Parliament, Council and member states will amend it until the text becomes law), we urge the Commission to clarify the questions below, and expand and refine requirements for transparency reporting and auditing.

### **Liability and the Updated Notice and Action System**

The main intention behind the DSA was to update the liability rules for online platforms, and we support its general approach of differentiated obligations for large and small platforms. Like many other civil society organizations, we were pleased that the

Commission's rules uphold the limited liability regime of the e-Commerce directive, and most importantly a ban on general monitoring obligation (also known as upload filters).

We also support the Commission's proposal to update the "notice and action" system with rules that empower users to settle disputes on the legality of content through independent "dispute settlement bodies." Nevertheless, we share partners' [concerns](#) that the text, in its current form, could place too much power with platforms for determining the legality of content, which would unintentionally lead to more automated filtering.

## **Transparency & Data Access for Research Scrutiny**

We know from our own work that existing transparency tools have [failed to provide watchdogs and regulators with the information they need](#) to hold platforms accountable for their impact on democratic processes and fundamental rights. As we have emphasized throughout our [Governing Platforms project](#), one of the key barriers to ensuring adequate transparency of algorithmic systems is the [lack of access to the data](#) that watchdogs need to scrutinize how very large platforms target, moderate, and recommend content or services to their users. We are thus very pleased to see that the Commission heeded civil society's calls for [legally binding data access frameworks](#) and [public access to advertisements repositories](#). Under the proposed rules, large platforms will be required to make available Application Programming Interfaces (APIs) that include information about advertisement content targeting criteria. Furthermore, vetted researchers will be able to apply to access platform data for the purposes of "conducting research that contributes to the identification and understanding of systemic risks," including potential negative effects on fundamental rights or civic discourse.

According to the draft, vetted researchers will be able to submit an application to the "European Board for Digital Services," a EU-wide supervisory body intended to advise national "Digital Services Coordinators" (existing national regulators) and the Commission on the enforcement of the DSA. After approval by the board, researchers will have access to online databases or APIs, providing that the request would not lead to "significant vulnerabilities." The [European Democracy Action Plan](#), which was released at the beginning of the month, further clarified that GDPR "does not prohibit the sharing of personal data by platforms with researchers," which is in line with [our research showing that user privacy and meaningful access can go hand in hand](#).

While we are thrilled that vetted academics will be provided with pathways to scrutinize data from large platforms, we are concerned that the rules limiting data access to academic institutions are overly restrictive. While it is crucial that data access provisions are privacy-respecting and GDPR compliant, we think it is vital that the proposed European Board also provides access to other stakeholders such as civil society and

journalists who play a key watchdog function. Despite these shortcomings, the provisions, if effectively enforced, could prove a big step forward for the academic and civil society communities who, up until now, have had to [jump through hoops](#) to access basic information about how large online platforms impact fundamental rights.

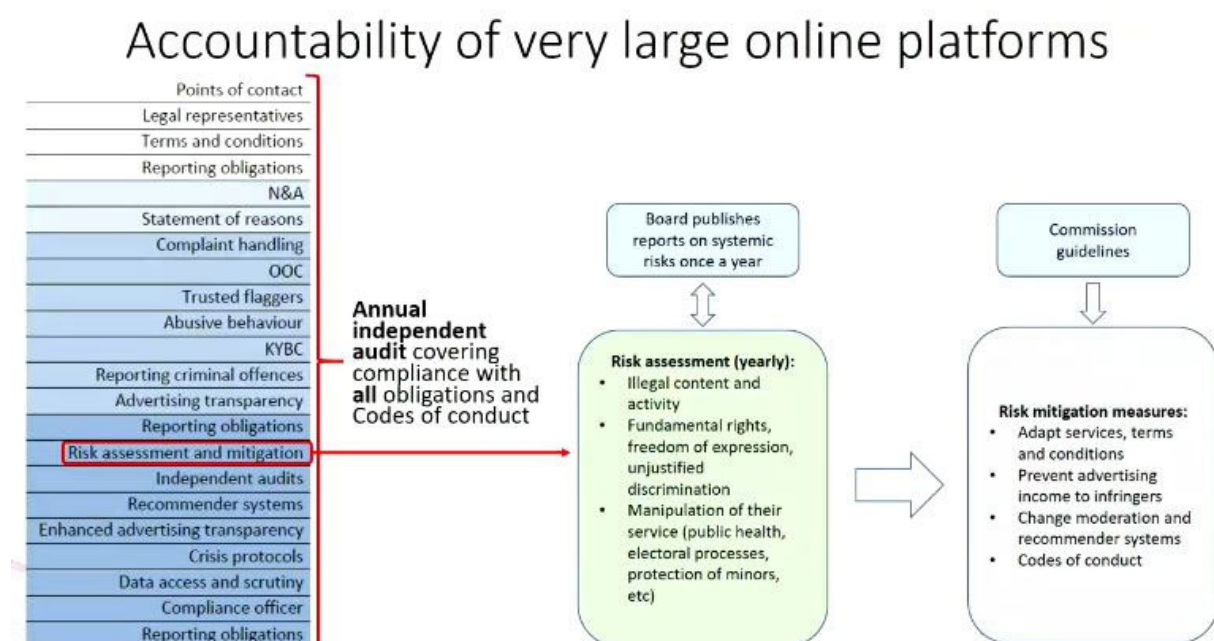
Nevertheless, transparency is only the first step. In order to hold platforms accountable, the DSA also needs to deliver on enforcing the rules of the game, which is why its proposed auditing rules are worth further scrutiny.

## Auditing and Enforcement

Alongside its provisions on improved transparency and data access for researchers, the Commission's draft calls for two additional layers of oversight for very large platforms: Audits by independent auditors and auditing powers for regulators. We welcome the Commission's approach and appreciate its proposal for such a comprehensive auditing and enforcement regime. However, enforcing such a system will be a complex task, and we have some questions about how these complexities will be dealt with.

### Audits by Independent Third-Party Auditors

But first things first, let us unpack the Commission's plan. According to the proposal, large platforms will undergo mandatory audits by independent auditors that have "expertise in the area of risk management," as well as "technical competence to audit algorithms." These auditors should ensure that large platforms are in compliance with a long list of obligations, ranging from rules on recommender system transparency to its updated notice and action rules. For a detailed overview of the proposed accountability mechanisms, see below:



*Source: European commission technical briefing*

Among the obligations for very large platforms is a requirement that companies conduct risk assessments to identify “significant systemic risks.” If the platform’s own risk assessment identifies threats to users’ safety, fundamental rights, public health or electoral processes, they will be required to take steps to mitigate these risks, including through voluntary cooperation in various codes of conduct (e.g. a revamped [Code of Practice on Disinformation](#)) or “crisis protocols.”

### Audits by Regulators

Independent third parties and researchers will not be the only ones who will be able to scrutinize platform compliance with the proposed rules. The draft also empowers member-state level “Digital Services Coordinators” with the authority to carry out onsite inspections. Upon recommendation of the European Board, the Commission can also conduct onsite investigations and request “access to, and explanations relating to, its databases and algorithms.”

### Enforcement, Baby!

This layered approach looks good, but what would it look like in practice? Does the Commission’s proposal provide individuals with adequate protections against abuses of power (both by platforms and by states)? The fact that very large companies would be required to conduct risk assessments is generally positive. Yet, because these are merely self-assessments, if auditors are not provided with concrete and meaningful criteria against which to evaluate such risk assessments, we might not see much more than a box ticking exercise. In general, the question of who audits or certifies the auditors remains open.

Furthermore, we are wary of the Commission’s overall emphasis on non-binding codes of conduct and “crisis protocols” as a means of demonstrating evidence of a platform’s “good faith” mitigation efforts. On the one hand, it makes sense that platforms be required to take concrete actions to mitigate systemic risks. At the same time, we are cautious that such arrangements could pave the way for abuses of power by governments keen to leverage the power of global companies for “emergency” quick fixes. As the current conflict [between Germany’s health ministry and publishers shows](#), the use of state influence to facilitate the “dissemination of reliable information” in emergencies can be somewhat of a slippery slope – even when the goal is to ensure the reliability of information during a pandemic.

If the GDPR has taught us anything, it is that the question of enforcement will be key. In order to deliver on its promises for increased transparency and accountability, national

regulators must be both willing and able to make use of their newly endowed regulatory toolbox. They must have clear and effective administrative procedures in place to deal with cross-border complaints, as well as the technical know-how to audit complex algorithmic systems.

The proposed regulation suggests that the Commission might have learnt from the GDPR experience, insofar as it provides for enhanced supervision mechanisms for very large platforms. In the event that national competent authorities either lack sufficient expertise or resources, or are unwilling to do so, the Commission itself can intervene. This underlines the Commission's ambition to crack down on Silicon Valley, but it remains to be seen whether or not this is sufficient.

## **Lastly, a Few Words on the Process**

The Commission prefaces its proposal with a note highlighting the results of its public consultation, which included a 270-question-long consultation questionnaire. According to the Commission, it received a whopping 2,863 responses and around 300 position papers from interested NGOs, companies/business associations, and individuals. AlgorithmWatch was among the relatively few civil society respondents, and while we were grateful for the opportunity to provide input into the process, the consultation process left much to be desired. The survey's highly technical nature made it extremely difficult to navigate, [especially for organizations representing impacted communities](#). Such a process drains NGOs of their already limited capacities, and privileges those organizations with the most legal and technical resources. In practice, this means private companies. We urge the Commission to consider more inclusive participatory instruments as well as [measures](#) that better support the principle of political equality in future consultation processes.

This is especially timely considering the lobby battle ahead. We are troubled by reports about the amount of resources that large tech platforms are pouring into their lobby efforts – both through direct and indirect channels. According to Politico's [most recent report](#), lobby efforts through private networks have only intensified as the scope of the DSA/DMA package became apparent, and the fact that lobby discussions have moved from public events to private WhatsApp or Twitter messages makes these activities much more difficult to scrutinize.

We fully agree with the Commission's proposal that very large online platforms should "design their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations." However, we are doubtful that this can be achieved by relying on its existing participatory toolbox. If the Commission wants

to succeed in taking platform governance decisions out of the boardroom, it must also address its own democratic shortcomings.