Mozilla position paper on the EU Digital Services Act

May 2021

Executive summary

Mozilla welcomes the European Commission's legislative proposal for a Digital Services Act. We were heavily involved in the policy discourse that preceded the DSA's publication, and are encouraged that many of our recommendations were incorporated into the draft law.

While the general policy approach of the DSA has merit, we nonetheless believe that many areas require clarification and further elaboration in order to be effective, and in order to protect the interests of individuals and challenger companies.

In this position paper we set out our perspectives and key recommendations for how lawmakers in the European Parliament and the EU Council could improve the DSA during its mark-up

stage.

Our position can be summarised as follows:

- **Asymmetric obligations for the largest platforms**
  - We welcome the DSA's approach of making very large platforms subject to enhanced regulation compared to the rest of the industry, but we suggest tweaks to the scope and definitions.
  - The definition of these so-called Very Large Online Platforms (VLOPs) shouldn't be based solely on quantitative criteria, but possibly qualitative (taking into account risk) as well, in anticipation of certain extraordinary edge cases where a service that meets that quantitative VLOP standard is in reality very low risk in nature.

- **Systemic transparency**
  - We welcome the DSA's inclusion of public-facing ad archive APIs and the provisions on access to data for public interest researchers.
  - We call for the advertising transparency elements to take into account novel forms of paid influence, and for the definition of 'public interest researchers' to be broader than just university faculty.

- **The risk-based approach to content responsibility**
  - We welcome this approach, but suggest more clarification on the *types* of risks to be assessed and *how* those assessments are undertaken.

- **Auditing and oversight**
  - We welcome the DSA's third-party auditing requirement but we provide recommendations on how it can be more than just a tick-box exercise (e.g. through standardisation; clarity on what is to be audited; etc).
  - We reiterate the call for oversight bodies to be well-resourced and staffed with the appropriate technical expertise.

Introduction

Mozilla is the Corporation behind the Firefox web browser, the Pocket "read-it-later" application, and other products and services that collectively are used by hundreds of millions of individuals around the world. Mozilla's parent company is a not-for-profit Foundation that focuses on fuelling the movement for a healthy internet through advocacy, research and philanthropy. Mozilla's work is grounded in our Manifesto - principles for what we believe the internet is and ought to be.

We have long considered the EU Digital Services Act (DSA) to be a crucial opportunity to implement an effective and rights-protective framework for content responsibility on the part of platforms operating in the EU. We thus welcome the European Commission's legislative proposal, and we consider it to set out the appropriate regulatory architecture for effective content responsibility and sectoral oversight. That said, we are conscious that there is much in the legislative proposal to be clarified and specified. Considerable amendments will be required to ensure the final text establishes an effective, balanced, and future-proof legal framework.

We firmly believe that if developed properly, the DSA can usher in a new global paradigm for tech regulation. At a time when lawmakers from Delhi to Washington DC are grappling with questions of platform accountability and content responsibility, the DSA is indeed a once-in-a-generation opportunity. In that context, we wish to set out our perspectives and recommendations on the elements of the draft law that we consider to be most important from a regulatory standard-setting perspective, notably:

- **Systemic transparency,** to assess risks and harms in the platform ecosystem;
- The **risk-based approach,** to enhance content responsibility;
- **Asymmetric regulation,** to safeguard competition and proportionality;
- **Polycentric oversight,** through competent regulators, third-party auditors, and empowered researchers.

The limited focus of this paper should not be understood as an endorsement of the other elements of the legislative proposal - we simply feel these are ones where our input is most useful and where the DSA has the potential for greatest impact.

Key legislative recommendations

Very Large Online Platforms (article 25)

1. Asymmetric oversight is a welcome step forward

We support the Commission's policy approach of asymmetric regulatory oversight of so-called 'Very Large Online Platforms'.

Today's ecosystem of consumer-facing internet services is far from homogenous. Many of the most pressing policy issues pertain to types of companies that constitute a small subset of the market in terms of scale and business practices. For instance, the risks of harm arising from an open content recommender system embedded in a platform used by hundreds of millions of Europeans is simply incomparable with the risks of harm posed by a small webshop, a blogging service, or any other instances of small and medium size services that make up the longtail of the internet in Europe. Indeed, the risks of harm from a handful of consumer-facing services today are distinct not merely in *degree* but also in *kind*, and as such, an asymmetric model of regulation is appropriate. Simply put, the greater the risk the greater the corresponding responsibility. The alternative approach - whereby all services are subjected to the same regulatory obligations within a 'one-size-fits-all' regulatory paradigm - belies the nature of the policy problems the DSA seeks to address while placing a regressive and disproportionate burden on the longtail of small and medium-sized services.

2. Consider adding qualitative criteria for consideration in extraordinary cases, to mitigate low-risk companies accidentally being caught in scope

We note that the draft law's definition of Very Large Online Platforms is determined solely on the basis of quantitative criteria. While we do not have substantive comments with respect to the chosen criteria (i.e. whether 10% of the Union population is too high or too low a metric), we are mindful that an exclusively-quantitative definition may bring into scope some online services not typically considered as posing significant content-related risks. Just as Very Large Online Platforms are distinct from the rest of the internet ecosystem, not all Very Large Online Platforms are the same. Content responsibility should be a function of risk - while size may be an important determinant of risk it is not the only one. To use the example of a content recommender system, a platform operating an 'open' system (e.g. Facebook 'News Feed') should have far greater risk management responsibilities than the operator of a 'curated' system (e.g. Spotify 'Made for You'), given that content in the former system is not subject to prior editorial control.

Fortunately, there are some relatively simple means by which the proportionality of obligations can be ensured. We note that the legislative proposal for a Digital Markets Act (DMA) likewise deploys quantitative criteria to designate the companies subject to regulation. However, the DMA mechanism also includes qualitative criteria as a secondary consideration, such that regulators can still designate a given company as having gatekeeper status if it does not meet the quantitative thresholds. This principle - in *inverse* form - should be deployed in the DSA approach to defining Very Large Online Platforms. As such, the primary and predominant criterion for designation would remain the quantitative thresholds outlined in article 25. However, the qualitative criteria outlined in recital 53 and 54 (e.g. reach; societal risk; etc) should be added to the operative article as factors that regulators could consider as mitigating factors that justify exclusion in extraordinary circumstances. For instance, a platform might reach the quantitative threshold for VLOP designation, but owing to its business model (e.g. all content on the platform is subject to editorial control) it does not pose significant societal risks as understood by the DSA. The DSA should provide a mechanism by which regulators can choose to waive VLOP-relevant obligations in these cases. Crucially, the qualitative considerations would only be appropriate to apply in *extraordinary cases*, and should only function as an elective means to exclude certain companies, not conditions that must be proven to exist for inclusion. To ensure the framework remains resilient and to limit backsliding, we view this qualitative criterion as a 'safety value' of sorts - never *intended* for use, but on hand for regulators to deploy in extraordinary cases.

Moreover, as a general consideration we believe it is essential that the obligations for Very Large Online Platforms in the DSA, and their subsequent oversight by regulatory authorities, be understood with reference to the principles of necessity and proportionality. We appreciate the draft DSA aims at this already, but it is a consideration that lawmakers must remain mindful of when proposing amendments

Key recommendations:

- Maintain the asymmetric regulatory regime for Very Large Online Platforms
- Amend the designation mechanism of Very Large Online Platforms such that it incorporates the qualitative criteria of recitals 53 and 54 into the operative article as mitigating factors for regulators in extraordinary circumstances.

Risk assessment and risk mitigation (articles 26-27)

As implied above, we support the draft DSA's risk-based approach to content responsibility. It is an approach that is more attuned to the problem of illegal and harmful content online, in that it can incentivise trust & safety measures that address *why and how* certain online experiences are *harmful* for individuals and groups.

To elaborate, harm is often a function of **scale**. For instance, while it is unfortunate if an individual conveys a mistruth about the safety of COVID-19 vaccinations to their family members, few would contend that an individual case of this kind is a *policy problem*. Yet if the same mistruth is posted on a social media network and is then amplified and micro-targeted to hundreds or thousands of other individuals through a content recommender system the calculus changes. In the case of COVID-19 mistruths the harm is typically not something intrinsic in the content, but rather the *reach* of that content. Harm is often a function of ***who* sees the content and under *what* circumstances.** For instance, self-harm content is likely to be most harmful if presented to vulnerable users in a manner that creates a sequential pathway towards increasingly more distressing content (e.g. Autoplay; Watch Next product features).

The risk-based approach can ensure that trust & safety compliance measures on the part of Very Large Online Platforms are responsive to this reality. It shifts attention away from content and towards the welfare of individuals using the service. Moreover, it compels Very Large Online Platforms to systematically consider how content-related risks are elevated or diminished by design and operational choices. This is a welcome improvement from the content-centric approach that has shaped previous legislative interventions, whereby 'responsibility' is assessed in terms of how much content is taken down, how many accounts are suspended, and how long it all takes. Assessing risks and mitigating harms, as opposed to scrubbing away bad content, is a sophisticated approach that reflects conditions in the world.

While we support the policy architecture of the risk-based approach as outlined in articles 26 and 27, we believe that both will require improvement in the mark-up stage. We outline the key improvements below.

1. ***Specify what risks to be assessed.***

The draft DSA insufficiently specifies the risks of *what* and to *whom* that Very Large Online Platforms ought to consider in their risk assessment.

Firstly, what risks are to be assessed. Article 26.1(b) directs service providers to take into account possible risks to individuals' rights under the EU Charter of Fundamental Rights without providing any specificity or substantive direction on how such an assessment against fundamental rights principles should be undertaken. While the Charter is an important bedrock, this present formulation is overly abstract and theoretical to serve as a basis for risk assessment. Consequently, we believe that article 26 should be amended such that it provides more clarity on the types of risks that Very Large Online Services should assess in their formal risk assessment. For instance, rather than simply being obliged to assess risks to how users can exercise their right to receive and impart information in general, Very Large Online Platforms should be obliged to

assess a minimum set of elaborated known risks that can engage the broad constitutional right to receive and impart information.

2. ***Account for collective and societal risks***

Secondly, by grounding risk assessment in the EU Charter of Fundamental Rights, the DSA's approach focuses risk assessments towards those risks that are likely to accrue to *individuals*. This focus on risks to individuals' rights is a welcome step forward and can help ensure a human-centric approach to platform responsibility. Yet we must not lose sight of the fact that many of the risks that we are most concerned with in the context of Very Large Online Platforms are *collective* and *social* in nature, for instance risks to public health; risks to social stability; risks to electoral integrity; etc. These are important risks that need to be assessed and managed, and crucially, they often only become visible on the basis of broad analysis through time. While we acknowledge that article 26.1 (c) takes a broader lens of risk, it is engaged only with respect to intentional manipulation by bad actors. The point is that we need to also consider these outcomes as being risks from the service operating *as intended*. In that context, risk assessment under the DSA should apply to both risks to individuals as well as collective and societal risks. This will ensure that the measures Very Large Online Platforms take to address risks on, through, and because of their services take account of the full range of downside issues that mark the contemporary online ecosystem.

3. ***Ensure efforts are aimed at probability of risks, not only the severity of the adverse outcome.***

Risk is generally understood as a function of the probability and severity of an adverse outcome. Across industries and operational domains, organisations that care about risk normally focus on managing *both* the probability and the severity of the adverse outcome. For instance, the fire safety function of an engineering firm will typically aim to ensure that its design both reduces the probability of a fire breaking out (through effective electrical current load-balancing; the use of fire-resistant cabling, etc) as well as the severity of any fire that may nonetheless break out (e.g. by installing fire doors and sprinkler systems). Simply put, once a risk has been identified the appropriate response is normally to try to manage both its probability and severity.

Unfortunately the DSA falls short in this respect, in that it is weighted heavily towards managing the *severity* of identified risks. For instance, article 26.1 (a) and (c) direct services to manage the risks associated with the dissemination of illegal content on their services and the risks associated with intentional manipulation of their service. As drafted this approach incentivises interventions that occur *after* the risk has materialised, such as the establishment of trusted flagger mechanisms or the deployment of automated filtering technology. While obviously necessary, these *ex post* mitigation measures are not sufficient. Rather, Very Large Online

Platforms must also assess and manage the *probability* of risk occurring through their services. This means taking into account the ways in which design choices and operational approaches can influence and increase risk. As a case in point, many social networks must contend with the risk that their service will amplify illegal hate speech. It is reasonable to assume that risk mitigation measures in this context should interrogate and seek to correct for the ways in which the service might be inadvertently amplifying this content owing to design and operational choices, and not simply focus on removing the proscribed content as a band-aid measure. On this basis, we recommend that lawmakers consider amendments that ensure risk assessment and management measures properly take into account the probability of risks occurring, particularly as they relate to service design and operation. This would force Very Large Online Platforms to 'price-in' societal risk to their business operations, so that the decision as to what to build and how to built it is not merely based on profit maximisation considerations that take no account of unforeseen downside risks (like the amplification of illegal and harmful content through content recommender systems). While it would not be appropriate for the DSA to define what 'good' design and operational architectures look like (e.g 'content recommender systems must promote authoritative content'), at the very least it should create the discentives to build products with hidden harms.

4. ***Risk assessments must be granular to be meaningful.***

The most worrying aspect of the DSA's risk-based approach is that it may well transpire to be a paper tiger - elegant and sound in theory, but ineffective in practice. This will be the case should the risk assessment and mitigation measures in articles 26 and 27 come to be mere box-ticking exercises and administrative formalities for Very Large Online Platforms operating in the EU. While this outcome is foreseeable based on the current DSA formulation, we are confident that it can be averted with targeted amendments and political will.

As a starting point, the DSA must ensure that risk assessments are specific and granular. In its current form, the DSA arguably only requires that *a* risk assessment of some form take place; that a figurative box be ticked. What is required is a specific framework to shape that risk assessment process and ensure that it meets an acceptable baseline of rigour. The recommendations we outline above can contribute to that process of textual elaboration. In addition, we encourage lawmakers to ground the DSA's risk assessment regime within existing international approaches to risk assessment and management, notably the ISO 31000 risk management standard.

Beyond this, the most effective means of ensuring that the risk-based approach translates into effective responsibility on the part of Very Large Online Platforms will be through a robust architecture of polycentric oversight underpinned by systemic platform transparency. As we explain in our comments on related articles below, the DSA risk-based approach should be

overseen by regulatory authorities that are well-resourced and empowered; third-party auditors that adhere to rigorous standards; and a distributed network of independent public interest researchers who can capitalise on the data access provisions of the DSA framework.

Key recommendations:

- Article 26 should be amended such that it provides more clarity on the types of risks that Very Large Online Services should assess in their formal risk assessment.
- Risks assessments undertaken pursuant to article 26 should apply to both risks to individuals as well as collective and societal risks.
- Lawmakers should consider amendments that ensure risk assessment and management measures properly take into account the probability of risks occurring, particularly as they relate to service design and operation.
- Lawmakers should consider whether and to what extent the DSA's risk assessment and mitigation regime can be grounded within existing international approaches to risk assessment and management, notably the ISO 31000 risk management standard.

Third-party auditing (article 28)

As noted above, third-party auditing can be an effective pillar of polycentric decentralised oversight of Very Large Online Platforms. Specialist auditors can provide broad scrutiny of platforms' compliance, supplying an oversight baseline that complements the efforts of regulatory authorities and ensures that public interest independent researchers can focus their attention on hidden harms and issues with disparate impact. That said, there are a number of considerations that EU lawmakers should be conscious of when considering article 28 of the legislative proposal.

1. Auditing regimes must be granular in nature

To be effective, the auditing regime must actually look 'under the hood' of Very Large Online Platforms, taking into account the design and operation of their systems as well as the risk mitigation measures that have been undertaken pursuant to the DSA provisions. As with the articles on risk assessment and risk mitigation, the draft DSA simply directs that a third-party audit be conducted, once again leaving open the possibility that the auditing process will descend

into a box-ticking exercise. To address this, the DSA should elaborate a non-exhaustive list of elements that ought to be audited under this provision, and direct regulatory authorities to update this guidance as market conditions evolve.

2. ***Explore standardisation and certification, to ensure a thriving and professionalised auditing market***

External auditing of content-sharing platforms is a fledgling industry that is presently lacking in professional standardisation or recognised certification mechanisms. One major concern we have is that by mandating third-party audits at a time when a robust and professionalised auditing industry is lacking, the DSA might stimulate the development of a sub-optimum market for auditing services. In addition to undermining the ability of auditing to contribute to the DSA's oversight mechanism, this state of affairs might give rise to a culture of 'ethics-washing' and turn the auditing regime into an exercise of corporate PR. There is already documented evidence of this phenomenon within the context of the emergent algorithmic auditing industry in the United States, and it is a risk that cannot be under-estimated in the DSA.

This can be mitigated in part by providing more specificity into what audit reports should contain and how they should be conducted by the relevant third-parties (e.g. where relevant, an analysis of a VLOP's content moderation process documentation; engagement metrics for recommended content that is subsequently found to violate the VLOP's ToS). In that endeavour, we encourage lawmakers to consider the recommendations put forward in the recent joint-report by the Ada Lovelace Institute and Reset. While it is likely inappropriate to seek to establish a durable audit standard in the DSA itself, the standardisation process foreseen in the DSA's article 35 could guide the development of the auditing industry in the EU and globally. That standard-setting endeavour should thus be pursued as a matter of priority once the DSA comes into effect.

3. ***Audit the auditors***

While third-party auditing is never a silver-bullet (and as such must be viewed as one pillar of a polycentric oversight architecture) it has proven relatively successful in sectors where the auditor and the entity to be audited are subject to *structurally misaligned* incentives. This does not simply mean that the auditor does not have a conflict of interest. Rather it means that the auditor is actually *incentivised* to rigorously assess the relevant company and its compliance with the DSA rulebook.

Unfortunately the DSA auditing regime does not build-in this misalignment of incentives, and worse, appears to undermine it. Notably, article 28 directs Very Large Online Platforms to submit themselves to a third-party audit by a provider of *their choosing* and at *their expense*. Assuming the market for auditing services is not monopolistic, auditors will likely compete for business

from platforms on the basis of price and service. And an obvious means of securing and retaining business will be through the furnishing of favourable auditing reports. As such, the auditing regime could deteriorate into an ineffective PR stunt, a risk that is likely to be compounded by the aforementioned lack of standardisation or certification within the emerging auditing industry.

Other domains have sought to build in a structural misalignment of incentives in the auditor-auditee relationship by leveraging the risk of litigation or regulatory sanction. For instance, in the financial services domain third-party auditors of publicly-listed companies can be sued by those companies' shareholders and sanctioned by the financial services regulator if they are negligent in carrying out their audit. Lawmakers should explore whether this approach could be borrowed to some extent in the DSA, for instance by building in a mechanism whereby regulatory authorities 'audit the auditors'.

Key recommendations:

- The DSA should elaborate a non-exhaustive list of elements that ought to be audited under this provision, and direct regulatory authorities to update this guidance as market conditions evolve.
- The DSA should direct regulatory agencies at EU-level to explore a standardisation process that could guide the development of the auditing industry in the EU and globally.
- Lawmakers should explore mechanisms for ensuring auditors act in the public interest and are subject to structurally misaligned incentives from those who they audit.

Recommender systems (article 29)

As has been noted at multiple points in this paper, we consider content recommender systems to be an important vector for online harms. For that reason we believe it is essential that the risk assessment and mitigation measures, as well as the provisions on third-party auditing and access to data for researchers, include content recommender systems within their scope of applicability. At the same time, the ever-more important role these systems play in shaping online experiences, and the ways in which they can engender unforeseen harm, means it is reasonable that the DSA gives dedicated attention to them through article 29.

Today many users of Very Large Online Platforms have little understanding or ability to influence the ways in which their content experiences are curated through recommender systems. This is a concerning state of affairs, given the prominence of these systems and the ways in which they can engender harm for users. At Mozilla, we are especially cognisant of the latter point, as our recent YouTube Regrets campaign uncovered harrowing stories of individuals who

experienced problematic content curation through recommender systems and who were often powerless to address or alter the curation logic.

On that basis, we support the article 29 (1) obligation for Very Large Online Platforms to provide meaningful transparency into targeting parameters that determine why users see specific content through recommender systems, and the obligation to offer users the ability to opt-out of recommendations that are based on personal data profiling. Taken together these provisions could encourage the industry to improve recommender system design and operation, and to place more emphasis on the needs and signals of the users of these systems.

However to be effective it is important that choice architectures and the user-facing transparency is meaningful, clear, and accessible. For that reason, we support the intent of article 29 (2), and recommend this to be an element that is audited as part of the article 28 third-party auditing mechanism.

Key recommendations:

- Maintain article 29 in its current form, and ensure it is complemented by risk management and auditing provisions elsewhere in the proposal that include recommender systems within their scope of applicability.

Transparency of online advertising (article 30)

The online advertising ecosystem remains a significant vector for the spread and impact of illegal and harmful content online. Yet before we can begin to advance effective policy solutions to address this still-emerging problem, we first need to understand precisely how and why the advertising ecosystem is being exploited.

In that context, the advertising transparency provisions of article 30 are a major step forward. They closely mirror the policy recommendations advanced by Mozilla and our allies in the lead-up to the DSA publication, most notably in that they concern all types of advertising and mandate the disclosure of key advertising targeting parameters. More information on why these features are so important can be found in our submission to the DSA public consultation.

The DSA prioritises application programming interfaces (APIs) as the technical mechanism for delivering transparency of advertising. While APIs have pragmatic appeal and are a useful mechanism of ensuring privacy and security, it should nonetheless be noted that this access model ensures some degree of power and control remains with the entity that offers the API. We

have seen many instances in the past of how this proprietary control has been used to frustrate or limit public interest research (e.g. by limiting API functionality or simply breaking it). It will thus be incumbent on national Digital Service Coordinators and the European Commission to ensure ad archive APIs function effectively and contain the data required for meaningful transparency.

Ultimately, we encourage lawmakers to resist calls to weaken article 30. Moreover, we believe that with a number of tweaks and clarifications, it can be made even more robust and future-proof in the face of a constantly-evolving advertising ecosystem. We list some of these recommendations below:

1. ***Account for user-generated paid-promotion***

We are also acutely aware that there are emergent forms of paid promotion that, while not directly-mediated by online services and not captured by the DSA's understanding of advertising, nonetheless pose similar kinds of risks to those associated with the online advertising ecosystem. In this regard we refer to 'user-generated paid promotion', by which we mean the phenomenon of actors directly paying service users (often, so-called 'influencers') to create content to promote a cause, belief, or brand. Despite not being financially-intermediated by the platform, and in operational terms interwoven into content rather than 'displayed' by the platform, paid promotion of this kind nonetheless engages similar policy issues and risks. A case-in-point is the efforts by former US Presidential candidate Michael Bloomberg to directly pay social media influencers to promote his electoral campaign.

We acknowledge that policy measures that are relevant for online advertising cannot be mirrored for user-generated paid-promotion of this kind. For a start, this form of content is user-generated and unlike advertising copy, it is not directly mediated and placed by the platform. As such, it is not feasible to expect that a platform can automatically and systematically identify this form of paid promotion and include it within the ad archive, without cooperation from content creators and other third parties.

That said, there are two measures that lawmakers can consider to address the policy issues associated with user-generated paid-promotion. First, article 30 should be amended so that Very Large Online Platforms are obliged to include a self-disclosure mechanism for users who contribute user-generated paid promotion on the platform. Once disclosed through this mechanism, the content in question would then be added to the platform's dedicated ad archive. Second, it is likely that much relevant content will not be disclosed under a self-disclosure mechanism, especially the type of problematic behaviour that is likely to engage policy concerns. In that context, undisclosed user-generation paid promotion should be referenced as a risk that Very Large Online Platforms need to consider as part of their article 26 and 27 risk assessment

and mitigation efforts. Mitigation measures would likely vary by platform, but could include the provision of flagging tools for users who encounter harmful paid promotion.

We are acutely aware that user-generated paid promotion is a nascent phenomenon, but it is one that is evolving rapidly and is vulnerable to the same kind of policy risks associated with platform-mediated advertising. Moreover, as regulatory interventions like the DSA bring ever-increasing scrutiny to the online advertising ecosystem, bad actors are likely to migrate to forms of paid influence that exist beyond the reach of transparency mandates. And as this phenomenon continues to evolve, we may well see fragmentation in regulatory approaches across jurisdictions (a concern that is already manifesting with respect to obligations on social media 'influencers' to disclose paid promotion). As such, it is likely a good candidate for the DSA's code of conduct mechanism (article 35). There would be value in bringing together the various stakeholder groups (e.g. platforms, brands, consumer protection groups, social media 'influencers') to gain a better understanding of the phenomenon, its policy risks, and to explore means by which greater transparency and accountability can be ensured beyond simply adding #ad to a piece of user-generated content.

Key recommendations:

- The DSA should account for the emerging phenomenon of 'user-generated paid promotion' by:
    - Amending article 30 so that Very Large Online Platforms are obliged to include a self-disclosure mechanism for users who contribute user-generated paid promotion on the platform.
    - Establishing undisclosed user-generation paid promotion as a risk that Very Large Online Platforms need to consider as part of their article 26 and 27 risk assessment and mitigation efforts.
- Once the final law is adopted, the European Commission should consider the phenomenon of 'user-generated paid promotion' as a candidate for a Code of Conduct under DSA article 35.

Data access and scrutiny (article 31)

The ability for oversight entities to 'look under the hood' of online services to understand and assess how their design and operational practices may be contributing to online harms is an essential component for accountability in the platform ecosystem. Likewise, data access is

essential if oversight entities are to be able to properly verify the assertions made by Very Large Online Platforms as evidence of their compliance with the DSA provisions.

We therefore welcome the broad applicability of this article, and we caution against efforts to circumscribe it or exclude certain operational components. The aim of this provision is to ensure accountability and facilitate research into online harms in the platform ecosystem. We should thus ensure that it provides a maximal framework, and then define the precise scope of data access requests on a case-by-case basis. These issues are simply too important to leave oversight bodies hamstrung in their information-gathering powers.

We likewise welcome the DSA's recognition that independent researchers have an important role to play in ensuring accountability in the platform ecosystem. Often it has only been through the painstaking research by poorly-resourced independent scholars and activists - in the face of an adversarial posture from platforms - that we have been able to learn about the hidden harms in the ecosystem. Providing a regulatory underpinning and safety net for these endeavours is thus an important step forward. That said, we would advise EU lawmakers to drop the requirement that vetted researchers must be affiliated with academic institutions (article 31.4). That provision is exclusionary and is likely to limit the scope of important research, particularly into online harms that disproportionately affect marginalised and underrepresented groups. Vetted researchers should be assessed on the basis of their expertise, their ability to implement the necessary privacy and data protection safeguards and protocols, and their commercial independence. While the academic community will likely supply many effective researchers, so too will the community of data journalists; public interest data scientists, and think tank researchers, to name just a few. Ultimately then, we do not believe affiliation with an academic institution needs or ought to be a condition for partake in the article 31 benefits.

While there is policy merit in ensuring meaningful access to platform data by a diverse body of public interest researchers, the corresponding privacy and security risks must be properly managed at all junctures. Article 31 (5) of the regulation directs the European Commission to adopt delegated acts that establish technical standards for data access as well as well as clarification for how research can be undertaken in a way that complies with relevant data protection rules. The development and implementation of these delegated acts must be an utmost priority, and should provide detailed clarity on the necessary privacy, security, and data protection protocols that must underpin research projects. The delegated acts should also provide clarity on how the European Commission and national Digital Services Coordinators can ensure rolling oversight of the regime and specific research initiatives. Simply put, trust is essential for the framework to succeed, and the delegated acts must ensure safeguards by design that protect against bad actors undermining that trust.

Key recommendations:

- Lawmakers should resist pressure to circumscribe or water down the data access provisions of article 31.
- Lawmakers should drop the requirement that vetted researchers must be affiliated with academic institutions.
- Lawmakers should develop, as a matter of priority, the necessary delegated acts that detail the specific operational and security technical standards for data access.

Codes of Conduct (article 35)

We do not expect that the DSA will solve all of the problems related to content responsibility - the problems we grapple with in five years time may well be different than those that we're principally concerned with today, and the types of business models that mark the tech landscape will almost certainly evolve. For this reason we have long-argued that the DSA ought to focus on establishing an effective and durable *paradigm* for content responsibility in the EU, rather than an rigid overly prescriptive rulebook that quickly becomes dated.

We believe that codes of conduct can play an important role in substantiating the DSA regulatory framework and ensuring that it remains durable and relevant through time. They can be particularly effective for bringing regulatory clarity to issues that affect a small subset of the internet economy or for which a unique set of measures and efforts is required. Put another way, codes of conduct under the DSA should be specific in scope - they should aim at addressing a well-defined and discrete problem in a way that complements the general regulatory regime. That focus on complementarity is essential and it means developing Codes with a risk-based approach and systemic transparency at the core. In our submission to the public consultation on the European Democracy Action Plan we provide dedicated recommendations for how codes of conduct should fit within the DSA paradigm, using the EU Code of Practice on Disinformation as a case-study.

Codes should be multi-stakeholder in nature, with civil society organisations, independent researchers, and groups representing relevant stakeholder interests being included in the development and implementation. For Codes to be effective, there must be clear and effective oversight on the part of regulatory authorities. Code participants should be expected to make clear, targeted commitments that are specific to their service, and their performance should be assessed on a recurring basis. By way of example, the EU Code of Practice on Disinformation includes commitments by the signatories to ensure the integrity of their services. Given that threats to integrity and the way they can be addressed are unique to every company (e.g. bots;

impersonation; etc) Codes of Conduct should encourage companies to set service-specific commitments and measurement criteria, which can then be assessed in a dedicated manner.

Finally, we believe that Codes of Conduct can be an important mechanism for providing legal certainty to regulated entities and alleviating the pressure on national regulatory bodies. They can provide support to companies that seek to implement compliance programmes within their operations, and allow for the sharing of best-practice and the development of industry trust & safety standards. We therefore recommend to maintain the existing approach envisaged by the draft DSA, whereby Code participation can be considered one possible means of expressing compliance with the DSA's substantive rules. Codes of conduct are only effective when they are developed on the basis of trust and understanding, and typically require the participation of a variety of stakeholders beyond just technology companies. An approach that *encourages* rather than compels participation would therefore be more suitable. This is not to say that the commitments made by companies that join a Code of Conduct cannot be made binding. It simply means that they should not be forced to *join* in the first place. At the same time, policymakers should ensure due diligence when inviting entities to join Codes of Conduct, to both ensure a diversity of perspectives and expert insights, and to mitigate harms related to 'astroturfing'.

Key recommendations:

- Codes of conduct under the DSA should be specific in scope - they should aim at addressing a well-defined and discrete content-related problem.
- Codes should be developed with a risk-based approach and systemic transparency at the core, such that they reinforce and are consistent with the general regulatory paradigm of the DSA.
- As is the case in the draft DSA, participation in a Code of Conduct should be considered a means but not a necessity for expressing compliance with the DSA's substantive provisions. Codes are most effective when participation is voluntary.

Oversight (Chapter IV, sections 1-3)

In principle, we support the DSA's intent to provide national regulatory authorities with more information-gathering and enforcement powers, as transparency is a crucial prerequisite to accountability. That said, more work needs to be done to clarify the interaction *between* Digital Service Coordinators, and the points at which the European Commission and Digital Services Coordinators in Member States other than the platform's country of establishment can engage in dedicated regulatory oversight.

Moveover, experience teaches us that the weaknesses in agency-led regulation in the EU is not always because regulators lack investigatory or enforcement powers, but rather because they lack the resources and political support to do their job effectively. We acknowledge that the draft DSA article 39 seeks to anticipate this by obliging Member States to ensure that regulatory bodies 'have adequate technical, financial and human resources to carry out their tasks'. While it is important to have this requirement asserted in the regulation, it is equally important that the European Commission be committed to *vindicating it in practice*, by holding to account Member States that systematically fail to adequately resource their regulatory authorities.

In addition, we strongly believe that for oversight to be effective it must be polycentric. There must be no 'single point of failure' and the success of the DSA's regime must not hinge on a single national regulatory authority being willing and able to do its job. The inclusion of provisions on third-party auditing; access to data for researchers; and codes of conduct is therefore a cause for optimism. However, it cannot be denied that national regulatory authorities are the 'first amongst equals' when it comes to regulatory oversight, and they have an obligation to ensure that the other mechanisms for oversight are set up for success. This means supporting and overseeing the development of an effective platform auditing ecosystem - marked by professional diligence and standardised certifications - and ensuring that independent researchers and the public-at-large are able to benefit from the systemic transparency provisions of the DSA (e.g. those concerning access to platform data and the public disclosure of online advertising).

Key recommendations:

- The oversight regime of the DSA requires that regulatory authorities are well-resourced and benefit from political support. Lawmakers should ensure that this assessment is a key consideration of the monitoring and evaluation mechanisms for the DSA framework.

Conclusion

These comments outline Mozilla's perspectives and recommendations on the elements of the DSA are most important for us and for which we can provide thought leadership. They are not intended to be exhaustive and we will continue to elaborate our perspectives as the EU discussions on the legislative proposal evolves.

Ultimately we believe that the DSA legislative proposal has lived up to its billing as a next generation approach to platform regulation. As such, rather than advocating for sweeping

changes, we believe that targeted amendments and clarifications are required to ensure it rises to meet the pressing policy challenge.

We look forward to working with EU lawmakers and the broader community of policy stakeholders to help realise a final legislative text that promotes a healthy internet that serves individuals and communities in the EU.

For more information please contact Owen Bennett, Senior Policy Manager, Mozilla Corporation (obennett@mozilla.com).