Contribution ID: 1ad6cb23-a986-4b8c-9a08-80d11e5b0d47
Date: 08/09/2020 09:40:01

Digital Services Act package: open public consultation

Fields marked with * are mandatory.

Introduction

The Commission recently announced a Digital Services Act package with two main pillars:

- first, a proposal of new and revised rules to deepen the Single Market for Digital Services, by increasing and harmonising the responsibilities of online platforms and information service providers and reinforce the oversight over platforms' content policies in the EU;
- second, ex ante rules to ensure that markets characterised by large platforms with significant network effects acting as gatekeepers, remain fair and contestable for innovators, businesses, and new market entrants.

T h i s c o n s u l t a t i o n

The Commission is initiating the present open public consultation as part of its evidence-gathering exercise, in order to identify issues that may require intervention through the Digital Services Act, as well as additional topics related to the environment of digital services and online platforms, which will be further analysed in view of possible upcoming initiatives, should the issues identified require a regulatory intervention.
The consultation contains 6 modules (you can respond to as many as you like):

1. **How to effectively keep users safer online?**
2. **Reviewing the liability regime of digital services acting as intermediaries?**
3. **What issues derive from the gatekeeper power of digital platforms?**
4. **Other emerging issues and opportunities, including online advertising and smart contracts**
5. **How to address challenges around the situation of self-employed individuals offering services through online platforms?**
6. **What governance for reinforcing the Single Market for digital services?**

Digital services and other terms used in the questionnaire

The questionnaire refers to **digital services** (or 'information society services', within the meaning of the E-Commerce Directive), as 'services provided through electronic means, at a distance, at the request of the user'. It also refers more narrowly to a subset of digital services here termed **online intermediary services**. By this we mean services such as internet access providers, cloud services, online platforms, messaging services, etc., i.e. services that generally transport or intermediate content, goods or services made available by third parties. Parts of the questionnaire specifically focus on **online platforms** – such as e-commerce marketplaces, search engines, app stores, online travel and accommodation platforms or mobility platforms and other collaborative economy platforms, etc.
Other terms and other technical concepts are explained in a glossary.

How to respond

Make sure to **save tour draft** regularly as you fill in the questionnaire. You can break off and return to finish it at any time. At the end, you will also be able to upload a document or add other issues not covered in detail in the questionnaire.

Deadline for responses

8 September 2020.

Languages

You can submit your response in any official EU language. The questionnaire is available in 23 of the EU's official languages. You can switch languages from the menu at the top of the page.

About you

* 1 Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish

- French
- Gaelic
- German
- Greek
- Hungarian
- Italian
- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* 2 I am giving my contribution as

- Academic/research institution
- Business association
- Company/business organisation
- Consumer organisation
- EU citizen
- Environmental organisation
- Non-EU citizen
- Non-governmental organisation (NGO)
- Public authority
- Trade union
- Other

* 3 First name

Owen

* 4 Surname

Bennett

* 5 Email (this won't be published)

obennett@mozilla.com

* 7 Organisation name

255 character(s) maximum

Mozilla Corporation

* 8 Organisation size

- ○ Micro (1 to 9 employees)
- ○ Small (10 to 49 employees)
- ○ Medium (50 to 249 employees)
- ◉ Large (250 or more)

9 What is the annual turnover of your company?

- ○ <=€2m
- ○ <=€10m
- ○ <= €50m
- ◉ Over €50m

10 Are you self-employed and offering services through an online platform?

- ☐ Yes
- ☑ No

16 Does your organisation play a role in:

- ☐ Flagging illegal activities or information to online intermediaries for removal
- ☐ Fact checking and/or cooperating with online platforms for tackling harmful (but not illegal) behaviours
- ☐ Representing fundamental rights in the digital environment
- ☐ Representing consumer rights in the digital environment
- ☐ Representing rights of victims of illegal activities online
- ☐ Representing interests of providers of services intermediated by online platforms
- ☑ Other

17 Is your organisation a

- [ ] Law enforcement authority, in a Member State of the EU
- [ ] Government, administrative or other public authority, other than law enforcement, in a Member State of the EU
- [ ] Other, independent authority, in a Member State of the EU
- [ ] EU-level authority
- [ ] International level authority, other than at EU level
- [x] Other

18 Is your business established in the EU?

- (•) Yes
- ( ) No

19 Please select the EU Member States where your organisation is established or currently has a legal representative in:

- ( ) Austria
- ( ) Belgium
- ( ) Bulgaria
- ( ) Croatia
- ( ) Cyprus
- ( ) Czechia
- ( ) Denmark
- ( ) Estonia
- ( ) Finland
- ( ) France
- ( ) Germany
- ( ) Greece
- ( ) Hungary
- ( ) Ireland
- ( ) Italy
- ( ) Latvia
- ( ) Lithuania
- ( ) Luxembourg
- ( ) Malta
- ( ) Netherlands
- ( ) Poland

- Portugal
- Romania
- Slovak Republic
- Slovenia
- Spain
- Sweden

20 Transparency register number

255 character(s) maximum

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

174457719063-67

* 21 Country of origin

Please add your country of origin, or that of your organisation.

- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Djibouti
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia

- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar /Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo

- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- **United States**
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara

- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Latvia
- Lebanon
- Lesotho
- Liberia
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- Yemen
- Zambia
- Zimbabwe

* 22 Publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

- **Anonymous**
  Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.
- **Public**
  Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

☑ I agree with the personal data protection provisions

I. How to effectively keep users safer online?

This module of the questionnaire is structured into several subsections:

First, it seeks evidence, experience, and data from the perspective of different stakeholders regarding illegal activities online, as defined by national and EU law. This includes the availability online of illegal goods (e.g. dangerous products, counterfeit goods, prohibited and restricted goods, protected wildlife, pet trafficking, illegal medicines, misleading offerings of food supplements), content (e.g. illegal hate speech, child sexual abuse material, content that infringes intellectual property rights), and services, or practices that infringe consumer law (such as scams, misleading advertising, exhortation to purchase made to children) online. It covers all types of illegal activities, both as regards criminal law and civil law.
It then asks you about other activities online that are not necessarily illegal but could cause harm to users, such as the spread of online disinformation or harmful content to minors.
It also seeks facts and informed views on the potential risks of erroneous removal of legitimate content. It also asks you about the transparency and accountability of measures taken by digital services and online

platforms in particular in intermediating users' access to their content and enabling oversight by third parties. Respondents might also be interested in related questions in the module of the consultation focusing on online advertising.

Second, it explores proportionate and appropriate responsibilities and obligations that could be required from online intermediaries, in particular online platforms, in addressing the set of issues discussed in the first sub-section.
This module does not address the liability regime for online intermediaries, which is further explored in the next module of the consultation.

1. Main issues and experiences

A. Experiences and data on illegal activities online

Illegal goods

1 Have you ever come across illegal goods on online platforms (e.g. a counterfeit product, prohibited and restricted goods, protected wildlife, pet trafficking, illegal medicines, misleading offerings of food supplements)?

- ○ No, never
- ○ Yes, once
- ○ Yes, several times
- ○ I don't know

3 Please specify.

3000 character(s) maximum

4 How easy was it for you to find information on where you could report the illegal good?

Please rate from 1 star (very difficult) to 5 stars (very easy)	☆ ☆ ☆ ☆ ☆

5 How easy was it for you to report the illegal good?

Please rate from 1 star (very difficult) to 5 stars (very easy)	☆ ☆ ☆ ☆ ☆

6 How satisfied were you with the procedure following your report?

Please rate from 1 star (very dissatisfied) to 5 stars (very satisfied)	☆ ☆ ☆ ☆ ☆

7 Are you aware of the action taken following your report?

- Yes
- No

8 Please explain

3000 character(s) maximum

9 In your experience, were such goods more easily accessible online since the outbreak of COVID-19?

- No, I do not think so
- Yes, I came across illegal offerings more frequently
- I don’t know

10 What good practices can you point to in handling the availability of illegal goods online since the start of the COVID-19 outbreak?

5000 character(s) maximum

Illegal content

11 Did you ever come across illegal content online (for example illegal incitement to violence, hatred or discrimination on any protected grounds such as race, ethnicity, gender or sexual orientation; child sexual abuse material; terrorist propaganda; defamation; content that infringes intellectual property rights, consumer law infringements)?

- No, never
- Yes, once
- Yes, several times
- I don’t know

18 How has the dissemination of illegal content changed since the outbreak of COVID-19? Please explain.

3000 character(s) maximum

19 What good practices can you point to in handling the dissemination of illegal content online since the outbreak of COVID-19?

3000 character(s) maximum

20 What actions do online platforms take to minimise risks for consumers to be exposed to scams and other unfair practices (e.g. misleading advertising, exhortation to purchase made to children)?

3000 character(s) maximum

21 Do you consider these measures appropriate?

- Yes
- No
- I don't know

22 Please explain.

3000 character(s) maximum

B. Transparency

1 If your content or offering of goods and services was ever removed or blocked from an online platform, were you informed by the platform?

- Yes, I was informed before the action was taken
- Yes, I was informed afterwards
- Yes, but not on every occasion / not by all the platforms
- No, I was never informed
- I don’t know

3 Please explain.

3000 character(s) maximum

4 If you provided a notice to a digital service asking for the removal or disabling of access to such content or offering of goods or services, were you informed about the follow-up to the request?

- Yes, I was informed
- Yes, but not on every occasion / not by all platforms
- No, I was never informed
- I don't know

5 When content is recommended to you - such as products to purchase on a platform, or videos to watch, articles to read, users to follow - are you able to obtain enough information on why such content has been recommended to you? Please explain.

3000 character(s) maximum

C. Activities that could cause harm but are not, in themselves, illegal

1 In your experience, are children adequately protected online from harmful behaviour, such as grooming and bullying, or inappropriate content?

3000 character(s) maximum

2 To what extent do you agree with the following statements related to online disinformation?

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/ No reply
Online platforms can easily be manipulated by foreign governments or other coordinated groups to spread divisive messages	○	◉	○	○	○	○
To protect freedom of expression online, diverse voices should be heard	○	◉	○	○	○	○
Disinformation is spread by manipulating algorithmic processes on online platforms	◉	○	○	○	○	○
Online platforms can be trusted that their internal practices sufficiently						

guarantee democratic integrity, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality.	○	○	○	◉	○	○

3 Please explain.

3000 character(s) maximum

Disinformation is a broad and complex phenomenon, and implicates public figures, political entities (governments and parties), and the media. However, it is undeniable that online platforms, in particular social media services that rely on algorithmic curation and micro-targeting of content, are themselves important vectors for disinformation.

A useful conceptual framework for understanding disinformation on social media platforms is the 'ABC' framework, developed by disinformation researcher and former Mozilla Foundation Fellow Camille Francois. The ABC framework defines disinformation on social media platforms as comprising deceptive Actors, manipulative Behaviour, and harmful Content. When considering policy responses to disinformation, it is essential that the European Commission engages with these three factors. Too often the policy response to disinformation focuses exclusively and excessively on the harmful content component (e.g. through filtering mandates or specific takedown obligations). The fact that these approaches ignore why and how disinformation spread on social media platforms explains why they have largely failed to comprehensively address the disinformation challenge.

Importantly, the ABC framework accounts for the way in which disinformation is the product of vulnerabilities in social media services' design and operational architectures. Often, the purveyors of disinformation seek to exploit the workings of automated curation algorithms (that tend to privilege various 'engagement' metrics) in order to amplify their messaging and reach new audiences. This exploitation can be achieved by deploying bot accounts or similar means of 'coordinated inauthentic behaviour'. Again, in order to be comprehensive, policy responses to disinformation on social media services must take into account how the problem depends on exploitation of specific characteristics of these services' design and operational architectures.

In addition, effective policy responses should be built on a strong evidence base. That evidence base should account for how the phenomenon of disinformation manifests in the online ecosystem, as well as the effectiveness of various platform responses to it. To build that evidence base we need transparency, and today, the level of transparency varies substantially and in some instances is insufficient. In that context, the DSA should establish a clear framework for transparency with respect to disinformation. In Section I.II, we provide guidance on what such a transparency framework would look like, specifically in the case of algorithmic recommender systems and online advertising.

4 In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of COVID-19? Please explain.

3000 character(s) maximum

5 What good practices can you point to in tackling such harmful activities since the outbreak of COVID-19?

3000 character(s) maximum

D. Experiences and data on erroneous removals

This section covers situation where content, goods or services offered online may be removed erroneously contrary to situations where such a removal may be justified due to for example illegal nature of such content, good or service (see sections of this questionnaire above).

1 Are you aware of evidence on the scale and impact of erroneous removals of content, goods, services, or banning of accounts online? Are there particular experiences you could share?

5000 character(s) maximum

The following questions are targeted at organisations.
Individuals responding to the consultation are invited to go to section 2 here below on responsibilities for online platforms and other digital services

3 What is your experience in flagging content, or offerings of goods or services you deemed illegal to online platforms and/or other types of online intermediary services? Please explain in what capacity and through what means you flag content.

3000 character(s) maximum

4 If applicable, what costs does your organisation incur in such activities?

3000 character(s) maximum

5 Have you encountered any issues, in particular, as regards illegal content or goods accessible from the EU but intermediated by services established in third countries? If yes, how have you dealt with these?

3000 character(s) maximum

6 If part of your activity is to send notifications or orders for removing illegal content or goods or services made available through online intermediary services, or taking

other actions in relation to content, goods or services, please explain whether you report on your activities and their outcomes:

- ☐ Yes, through regular transparency reports
- ☐ Yes, through reports to a supervising authority
- ☐ Yes, upon requests to public information
- ☐ Yes, through other means. Please explain
- ☐ No , no such reporting is done

8 Does your organisation access any data or information from online platforms?

- ☐ Yes, data regularly reported by the platform, as requested by law
- ☐ Yes, specific data, requested as a competent authority
- ☐ Yes, through bilateral or special partnerships
- ☐ On the basis of a contractual agreement with the platform
- ☐ Yes, generally available transparency reports
- ☐ Yes, through generally available APIs (application programme interfaces)
- ☐ Yes, through web scraping or other independent web data extraction approaches
- ☐ Yes, because users made use of their right to port personal data
- ☐ Yes, other. Please specify in the text box below
- ☐ No

10 What sources do you use to obtain information about users of online platforms and other digital services – such as sellers of products online, service providers, website holders or providers of content online? For what purpose do you seek this information?

3000 character(s) maximum

11 Do you use WHOIS information about the registration of domain names and related information?

- ○ Yes
- ○ No
- ○ I don't know

13 How valuable is this information for you?

Please rate from 1 star (not particularly important) to 5 (extremely	☆☆☆☆

important)

14 Do you use or ar you aware of alternative sources of such data? Please explain.

3000 character(s) maximum

The following questions are targeted at online intermediaries.

A. Measures taken against illegal goods, services and content online shared by users

1 What systems, if any, do you have in place for addressing illegal activities conducted by the users of your service (sale of illegal goods -e.g. a counterfeit product, an unsafe product, prohibited and restricted goods, wildlife and pet trafficking - dissemination of illegal content or illegal provision of services)?

- [x] A notice-and-action system for users to report illegal activities
- [ ] A dedicated channel through which authorities report illegal activities
- [ ] Cooperation with trusted organisations who report illegal activities, following a fast-track assessment of the notification
- [ ] A system for the identification of professional users ('know your customer')
- [x] A system for penalising users who are repeat offenders
- [ ] A system for informing consumers that they have purchased an illegal good, once you become aware of this
- [x] Multi-lingual moderation teams
- [ ] Automated systems for detecting illegal activities. Please specify the detection system and the type of illegal content it is used for
- [x] Other systems. Please specify in the text box below
- [ ] No system in place

2 Please explain.

5000 character(s) maximum

Mozilla does not operate a platform to facilitate the sale of goods, and few of our services facilitate the hosting and sharing of third-party content. As such, illegal and harmful content are not phenomena we must deal with often.

That said, we have developed general Conditions of Use, and these proscribe particular forms of content and activity on our content-hosting and sharing services like AMO and Firefox Send. For instance, under our conditions of use, individuals cannot use services like Firefox Send or AMO to engage in activity that amounts to harm or exploitation of children; any effort to sell, purchase, or advertise illegal goods or services; etc. Failure to comply with these Conditions of Use can result in content removal or user

suspension, as relevant for the particular service.

In addition to the general Conditions of Use, we have also developed Community Participation Guidelines that apply to our internal, volunteer, contributor, and developer spaces online (e.g. the Mozilla Web Developers network; the Mozilla Community Portal; etc). The Community Participation Guidelines reflect our commitment to open, collaborative, and community-led discourse, while affirming our aim to promote and elevate civil discourse, critical thinking, and human dignity. To that end, the Community Participation Guidelines set our expectations of members of Mozilla's broad community in how they approach community interaction, and establish a set of consequences, up to and including sanctioning mechanisms for parties who initiate or participate in damaging behaviour.

Moreover, we have developed specific policies and user reporting functions concerning extensions and add-ons for the Firefox web browser. Every extension and theme distributed for use in Firefox is subject to Mozilla's add-on policies, which also require compliance with the Conditions of Use for Mozilla services. These policies and conditions have been created to protect users from inappropriate content or behavior in extensions and themes for Firefox. For instance, our policies prohibit add-ons or extensions that concern hateful, violent, sexual, or otherwise illegal content.

Finally, our Pocket read-it-later application deploys human curation methods to surface journalistic content that is worthy of its users time. Given the architecture of this service, illegal or harmful content is not a major concern but we nonetheless adhere to strict and detailed editorial guidelines to ensure that curated content maintains the highest standards of accuracy and quality. Moreover, as a bulwark against any potential harm, Pocket provides user-reporting functionality in the event that the community deems certain curated journalistic content to be harmful or potentially illegal.

3 What issues have you encountered in operating these systems?

5000 character(s) maximum

We have found our policies to be durable through time and sufficiently flexible to deal with the rare issues of illegal and ToS-violating content and activities arising on our properties. We have no particular issues to report.

4 On your marketplace (if applicable), do you have specific policies or measures for the identification of sellers established outside the European Union ?

- Yes
- No

5 Please quantify, to the extent possible, the costs of the measures related to 'notice-and-action' or other measures for the reporting and removal of different types of illegal goods, services and content, as relevant.

5000 character(s) maximum

6 Please provide information and figures on the amount of different types of illegal content, services and goods notified, detected, removed, reinstated and on the

number or complaints received from users. Please explain and/or link to publicly reported information if you publish this in regular transparency reports.

5000 character(s) maximum

Mozilla does not operate a platform to facilitate the sale of goods, and few of our services facilitate the hosting and sharing of third-party content. As such, illegal and harmful content are not phenomena we must deal with often.

Nonetheless, transparency is a key part of how Mozilla approaches user trust. As an open source project that relies on open development, we build transparency into the way we write our code. Additionally, our product documentation and notices describe how our products work and how we handle user data.

With this in mind, we publish bi--annual transparency reports that help provide additional transparency to government disclosures and content takedown requests.

Given the nature of our services, the categories of content takedowns that we report on tend to contain low numbers. For instance, in the period 1 July 2019 - 31 December 2019 (the latest period for which we have published a transparency report) we received three copyright takedown notices and six trademark takedown notices. We received no government requests to remove user content.

Our transparency reports can be accessed here: https://www.mozilla.org/en-US/about/policy/transparency/

7 Do you have in place measures for detecting and reporting the incidence of suspicious behaviour (i.e. behaviour that could lead to criminal acts such as acquiring materials for such acts)?

3000 character(s) maximum

Mozilla does not operate a platform to facilitate the sale of goods, and few of our services facilitate the hosting and sharing of third-party content. As such, illegal and harmful content are not phenomena we must deal with often.

As per our statutory obligations in the United States, we report any instances of child sexual abuse material or exploitation that we identify on our services directly to the US National Center for Missing and Exploited Children's CyberTipline.

B. Measures against other types of activities that might be harmful but are not, in themselves, illegal

1 Do your terms and conditions and/or terms of service ban activities such as:

- ☐ Spread of political disinformation in election periods?
- ☐ Other types of coordinated disinformation e.g. in health crisis?
- ☑ Harmful content for children?
- ☑ Online grooming, bullying?
- ☑ Harmful content for other vulnerable persons?
- ☑ Content which is harmful to women?

- [x] Hatred, violence and insults (other than illegal hate speech)?
- [ ] Other activities which are not illegal per se but could be considered harmful?

2 Please explain your policy.

5000 character(s) maximum

Please refer to our response to question A2 above regarding the applicability of Mozilla's policies.

3 Do you have a system in place for reporting such activities? What actions do they trigger?

3000 character(s) maximum

Mozilla does not operate a platform to facilitate the sale of goods, and few of our services facilitate the hosting and sharing of third-party content. As such, illegal and harmful content are not phenomena we must deal with often.

That said, we have developed a dedicated reporting function for any third-party extensions or themes for Firefox that may violate our general conditions of use or our Community Participation Guidelines. Extensions and themes can be directly reported in the Firefox web browser or in our add-ons store (addons.mozilla.org). In the event that an extension or theme is judged by our review team to be violating the above terms, it is removed from our add-ons store until the developer of the add-on addresses the issues. Depending on the history and severity of the abuse (particularly if it poses a security or privacy risk), the add-ons team may take action that prevents the extension or theme from loading in Firefox.

Mozilla's Community Participation Guidelines prohibit a number of these types of activities, content, and behaviours within Mozilla's spaces for staff, volunteers, contributors, and developers. To ensure these guidelines and conditions have practical force, we operate a dedicated web form hotline that allows our community or service users to report potential violations. These reports are triaged by the Community Participation Guidelines Response Lead. Depending upon the type of report and whether any Mozilla staff are alleged to be involved, a HR People Partner, employment counsel or the Chief Legal Officer may assume the report for review and investigation. The precise actions and outcomes arising from a complaint will depend on the nature and severity of the issue. Some reports trigger further investigation, private consultation, mediation, or a suspension of community participation.

Our Pocket read-it-later application is a manually curated service, and as such, the risk of harmful content circulating and impacting users is low. Nonetheless, we offer a reporting function where users can notify our editorial team of content that they consider problematic or harmful. Our editorial team will then review the article in line with our editorial guidelines and if necessary, remove it from our curated recommendation feed.

4 What other actions do you take? Please explain for each type of behaviour considered.

5000 character(s) maximum

5 Please quantify, to the extent possible, the costs related to such measures.

5000 character(s) maximum

6 Do you have specific policies in place to protect minors from harmful behaviours such as online grooming or bullying?

- (●) Yes
- ( ) No

7 Please explain.

3000 character(s) maximum

Our Conditions of Use apply to Mozilla's content hosting and sharing services, and prohibit their use to exploit or harm children. They also prohibit any use that seeks to threaten or harassess others, including minors.

C. Measures for protecting legal content goods and services

1 Does your organisation maintain an internal complaint and redress mechanism to your users for instances where their content might be erroneously removed, or their accounts blocked?

- (●) Yes
- ( ) No

2 What action do you take when a user disputes the removal of their goods or content or services, or restrictions on their account? Is the content/good reinstated?

5000 character(s) maximum

In our experience, this situation is relevant in the copyright domain. In general, Mozilla would restore challenged content where a user sends a counter-notice that complies with the requirements of the US Digital Millennium Copyright Act (DMCA). Mozilla would decline to restore the content, however, if the counter-notice purports to meet the requirements of the DMCA but appears to be abusive (e.g. it includes an obviously fake name and address)

3 What are the quality standards and control mechanism you have in place for the automated detection or removal tools you are using for e.g. content, goods, services, user accounts or bots?

3000 character(s) maximum

We do not use automated detection or removal tools for the purposes indicated above.

4 Do you have an independent oversight mechanism in place for the enforcement of your content policies?

- ( ) Yes
- (●)

No

5 Please explain.

5000 character(s) maximum

Given the nature of our services and their function, allied with the fact that we have had relatively few issues with illegal and harmful content in the past, we do not see a need for any additional independent oversight of the enforcement of our content policies. Moreover, we have not received any indication for our community or user base that additional oversight may be desired.

D. Transparency and cooperation

1 Do you actively provide the following information:

- [x] Information to users when their good or content is removed, blocked or demoted
- [x] Information to notice providers about the follow-up on their report
- [ ] Information to buyers of a product which has then been removed as being illegal

2 Do you publish transparency reports on your content moderation policy?

- (•) Yes
- ( ) No

3 Do the reports include information on:

- [ ] Number of takedowns and account suspensions following enforcement of your terms of service?
- [ ] Number of takedowns following a legality assessment?
- [x] Notices received from third parties?
- [ ] Referrals from authorities for violations of your terms of service?
- [x] Removal requests from authorities for illegal activities?
- [x] Number of complaints against removal decisions?
- [ ] Number of reinstated content?
- [ ] Other, please specify in the text box below

4 Please explain.

5000 character(s) maximum

Please see our response to question A6

5 What information is available on the automated tools you use for identification of illegal content, goods or services and their performance, if applicable? Who has access to this information? In what formats?

5000 character(s) maximum

With the specific exception of malware detection for submissions to our add-ons store, we do not use automated detection or removal tools for the purposes indicated above.

6 How can third parties access data related to your digital service and under what conditions?

- ☐ Contractual conditions
- ☐ Special partnerships
- ☐ Available APIs (application programming interfaces) for data access
- ☐ Reported, aggregated information through reports
- ☐ Portability at the request of users towards a different service
- ☐ At the direct request of a competent authority
- ☐ Regular reporting to a competent authority
- ☑ Other means. Please specify

7 Please explain or give references for the different cases of data sharing and explain your policy on the different purposes for which data is shared.

5000 character(s) maximum

As part of our commitment to ethical data and working in the open, we publish the Firefox Public Data Report, a weekly public overview on the activity, behavior, and hardware configuration of Firefox users.

The purpose of the report is two-fold:

Empowerment: We want to empower developers, journalists, and the overall public to better understand the state of the web and the direction of trends in web browsing.
Transparency: At Mozilla, we like to say that we are 'Open by Design'. We believe in an open web, so data and insights from the public should be made public, so the public can benefit.

The Firefox Public Data report publishes non-sensitive telemetry data that we gather from individual Firefox installations, including data on the browser's performance, hardware, usage and customizations. All data undergoes an extensive review process to ensure that anything we collect is necessary and secure.

With this data, we aggregate metrics for a variety of use cases, from tracking crash rates to answering specific product questions (e.g. how many clients have add-ons? 33% at last count.) In addition we measure the impact of experiments that we run to improve the browser. We make this data available to the public in a clear and intelligible manner because we recognise the power of open data in advancing research and innovation. For instance, to show what an internet outage looks like, we've recently released an aggregate open dataset on Italy's mid-pandemic internet outage. We've also published novel data from our telemetry datasets to advance research around the efficacy of social distancing measures to combat the spread of the COVID-19 pandemic. The data captured changes to Firefox users' engagement over time, a potentially

useful source of insight for researchers seeking to understand changes in individuals' daily habits as a means of understanding the impact of social distancing measures.

We believe the ethos underpinning the Firefox Public Data Report, and the operational principles underpinning it, are an important case study in how open data can advance the public interest while maintaining trust and privacy.

The following questions are open for all respondents.

2. Clarifying responsibilities for online platforms and other digital services

1 What responsibilities (i.e. legal obligations) should be imposed on online platforms and under what conditions?
Should such measures be taken, in your view, by all online platforms, or only by specific ones (e.g. depending on their size, capability, extent of risks of exposure to illegal activities conducted by their users)? If you consider that some measures should only be taken by large online platforms, please identify which would these measures be.

	Yes, by all online platforms, based on the activities they intermediate (e.g. content hosting, selling goods or services)	Yes, only by larger online platforms	Yes, only platforms at particular risk of exposure to illegal activities by their users	Such measures should not be required by law
Maintain an effective 'notice and action' system for reporting illegal goods or content	◉	○	○	○
Maintain a system for assessing the risk of exposure to illegal goods or content	◉	○	○	○
Have content moderation teams, appropriately trained and resourced	○	◉	○	○
Systematically respond to requests from law enforcement authorities	○	○	○	◉
Cooperate with national authorities and law enforcement, in accordance with clear procedures	○	○	○	◉

Cooperate with trusted organisations with proven expertise that can report illegal activities for fast analysis ('trusted flaggers')	○	◉	○	○
Detect illegal content, goods or services	○	○	○	◉
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law	○	◉	○	○
Request professional users to identify themselves clearly (‘know your customer’ policy)	○	◉	○	○
Provide technical means allowing professional users to comply with their obligations (e.g. enable them to publish on the platform the pre-contractual information consumers need to receive in accordance with applicable consumer law)	○	◉	○	○
Inform consumers when they become aware of product recalls or sales of illegal goods	○	◉	○	○
Cooperate with other online platforms for exchanging best practices, sharing information or tools to tackle illegal activities	○	○	○	◉
Be transparent about their content policies, measures and their effects	◉	○	○	○
Maintain an effective ‘counter-notice’ system for users whose goods or content is removed to dispute erroneous decisions	◉	○	○	○
Other. Please specify	○	○	○	○

2 Please elaborate, if you wish to further explain your choices.

5000 character(s) maximum

The DSA should serve as a broad framework whereby companies are empowered, incentivised, and held accountable for taking trust & safety measures commensurate with their means and their risk-profile. This framework should be built around two foundational pillars:

Procedural accountability:

Measures aimed at ensuring ‘responsibility’ should focus on improving platforms’ trust and safety processes and practices, rather than forcing them in vain to perfectly suppress illegal or harmful content. For instance,

policy interventions could encourage enhancements to flagging systems (e.g. more user-friendly reporting portals, increased proportion of local-language content moderators) or improvements to the means by which content is surfaced to users (e.g. greater transparency and auditing of algorithmic recommender systems). Similarly, the DSA framework could incentivise collaborations with expert organisations that streamline content detection (so-called 'trusted flaggers') or commercial tweaks to address systematic service abuses (e.g. demonetising the purveyors of illegal hate speech.) Importantly, this approach places the emphasis on making responsibility manifest in the practices and processes, and ensuring that they are appropriately attuned to content-related risks. Moreover, its metric of success is not content removal or account suspensions, but rather demonstrated policy structures and risk mitigation strategies. As such, this 'procedural accountability' ensures interventions happen where they are likely to have the most impact in addressing and mitigating harm, but in a way that does not necessitate companies to aggressively interfere with their users' fundamental rights.

A sliding scale of responsibility:

Content responsibility should be defined through principles whose application adjusts depending on the scale, risk-profile, or function of a service, rather than through one-size-fits-all rules. For example, a small startup with minimal user-generated content needs different moderation practices than a publication platform aimed at children or extremist groups. Likewise, an algorithmic recommender system that selects, amplifies, and micro-targets user-generated content should be subject to greater risk mitigation and trust & safety processes than a service that merely allows third-parties to share user-generated content. The alternative approach - as exemplified in the EU Copyright directive and the EU Terrorist Content regulation - establishes generalised rules that take no account of the various contextual factors (such as size, risk profile, and technical architecture) that determine what is a 'responsible' approach in reality. The consequence of this generalised approach is a compliance standard that only the largest companies can meet, and a greater risk of companies interfering with their users' fundamental rights in order to avoid sanction. The promise of a clearly-defined principles-based approach is that it would bring much-needed proportionality in the regulatory regime, and ensure that platforms address illegal content in a way which is reflective of their risk-profile, their technical architecture, and their resources.

In any case, we are wary of regulation prescribing specific measures or practices for platforms to express their 'responsibility'. While we believe many of the measures in the above table would be appropriate for large platforms to undertake in some form, we do not consider it to be practical for the law to prescribe them specifically.

An overly-prescriptive regime is likely to give rise to the problematic scoping issues (how to define who in scope versus who is out of scope) that were so prominent in the recent debate around the EU Copyright directive. Moreover, an overly-prescriptive approach is inappropriate given the heterogeneity of the platform economy and the fact that each platform requires tailored responses to trust & safety issues. Simply put, defining specific and broadly-applicable measures for platforms to express responsibility is unlikely to be sustainable in the long-run and a sub-optimum trust & safety response for the majority of platforms.

3 What information would be, in your view, necessary and sufficient for users and third parties to send to an online platform in order to notify an illegal activity (sales of illegal goods, offering of services or sharing illegal content) conducted by a user of the service?

- [x] Precise location: e.g. URL
- [x] Precise reason why the activity is considered illegal
- [x] Description of the activity
- [x] Identity of the person or organisation sending the notification. Please explain under what conditions such information is necessary:
- [ ] Other, please specify

4 Please explain

3000 character(s) maximum

As a general rule, the more information that helps identify the infringement or establish rights that a notification provides the better.

Information relating to the exact location of the infringement (e.g. a URL, an account handle) can ensure trust & safety teams can rapidly identify and act on the report. Moreover, information on what infringement is alleged is an important means of triaging reports and ensuring they are dealt with by the appropriate internal stakeholders and with due regard to their priority. Finally, information as to the identity of the reporter is particularly important in the context of IPR infringements, to ensure the reporter's rights can be established and, if relevant, to facilitate a counter-notice procedure.

Many platforms have developed specific reporting portals to ensure that the relevant information above/ additional information relevant to their specific trust & safety program is provided by reporters in a structured manner.

5 How should the reappearance of illegal content, goods or services be addressed, in your view? What approaches are effective and proportionate?

5000 character(s) maximum

In recent years, some of the largest platforms have developed technological solutions that aim at minimising reappearance. Examples include Microsoft's PhotoDNA (for child sexual abuse material), and YouTube's Content ID (for copyright-protected material). We urge the European Commission to be cautious in how it views these technological solutions. In recent years there has been a growing belief that automated filtering and hashing technologies can be a panacea for addressing reappearance and in the fight against illegal content generally. The problem is that these technologies cannot determine context or similarity, and for most assessments of illegality context is a key determinant. While these technologies may be relatively useful in addressing the reappareance of child sexual abuse material (CSAM) - where there is no context in which the content could be legal - they are inappropriate for combatting copyright infringement or hate speech, given the fundamental role played by the context of use in determining illegality.

For that reason, we urge the European Commission to refrain from mandating automated solutions to address the problem of reappearance, and moreover, where such solutions are deployed by platforms voluntarily, the Commission should consider means by which greater due process and transparency can be incorporated into the use of such technologies.

6 Where automated tools are used to detect illegal content, goods or services, what opportunities and risks does their use present as regards different types of illegal activities and the particularities of the different types of tools?

3000 character(s) maximum

As we outline in our response to question five above, automated tools are not a panacea in the fight against illegal content, goods, or services and they may potentially interfere with individuals' fundamental rights. At a minimum then, automated tools should not be mandated by law.

However, we acknowledge that some private actors - especially large social media services - are increasingly relying on automated content control technologies as a core feature of their trust and safety programme. The voluntary use of such technologies can fit within "content moderation at scale" only if their deployment is accompanied by meaningful oversight, accountability, and appeal mechanisms. To that end, we encourage the Commission to consider means by which more effective due process could be ensured where automated content moderation technologies are deployed in the market. Recommendations on how to ensure that due process can be found in the recently-published Santa Clara Principles (https://santaclaraprinciples.org). Moreover, we encourage the Commission to consider means by which companies of a certain size and impact could publish meaningful transparency reports that illustrate the extent to which automated content recognition technologies are deployed and their contribution to overall content moderation efforts.

7 How should the spread of illegal goods, services or content across multiple platforms and services be addressed? Are there specific provisions necessary for addressing risks brought by:

a. Digital services established outside of the Union?
b. Sellers established outside of the Union, who reach EU consumers through online platforms?

3000 character(s) maximum

We do not have particular recommendations with respect to digital services located outside of the EU.

8 What would be appropriate and proportionate measures for digital services acting as online intermediaries, other than online platforms, to take – e.g. other types of hosting services, such as web hosts, or services deeper in the internet stack, like cloud infrastructure services, content distribution services, DNS services, etc.?

5000 character(s) maximum

When considering what level of the internet stack to target content regulation interventions, the European Commission should abide by two foundational principles:

- Content control obligations should focus on intermediaries and layers of the stack that enjoy greatest proximity to the relevant content; and,
- Obligations to address illegal content should engender the least interference with lawful speech as

possible.

In practice, this means that the focus of intervention should be aimed at content-hosting services. As the host of the illegal content in question, hosting services enjoy the greatest proximity to it and they can make direct interventions to remove it or disable access to it. Further, this proximity means they can most precisely target the specific content, minimising the risk of over-removal, and thereby satisfying the second principle above.

As a corollary, services operating 'deeper' in the internet stack should not be subject to content control obligations. This means passive network intermediaries such as browsers, Internet Service Providers, DNS providers, Content Delivery Networks, cloud service infrastructure. These layers of the stack are inappropriate for content regulation, and applying such a regime to these intermediaries would both be ineffective and give rise to acute interferences with fundamental rights.

For instance, the Firefox web browser is a user-agent that performs an intermediary web rendering function. Blocking access to illegal content through Firefox would be grossly disproportionate; as a gateway to the entire Internet, such filtering will be rife with false positives that result in blocking of legitimate content. Moreover, the technical architecture of the internet is designed to route around blockages, and browser- and ISP-level blocking can be easily circumvented with the most basic digital skills. In that context, removal of illegal content at source i.e. from the services of the relevant hosting provider - is the only tenable approach that should be considered by the EU.

Today, some EU Member States require internet service providers to implement blocking and filtering measures to address illegal content. This is deeply regrettable, given how blocking at that level of the stack poses acute interferences with fundamental rights and is easily circumvented. With respect to EU Member States that engage in such practices, the European Commission should push for it to be underpinned by a clear legal basis and be subject to independent oversight and transparency.

9 What should be the rights and responsibilities of other entities, such as authorities, or interested third-parties such as civil society organisations or equality bodies in contributing to tackle illegal activities online?

5000 character(s) maximum

Public authorities should be subject to clear transparency requirements when they issue content takedown notices to digital services. These transparency requirements should ensure that public authorities provide clarity on what content is requested for removal; the motivation for the removal request; and the legal basis on which the request stands. This transparency is a key means of ensuring trust in public authorities and protecting against arbitrary and unjustified interference with fundamental rights.

In addition, public authorities should refrain from issuing content 'referrals' to digital services. This increasingly-common practice - whereby governments refer notices of legal-but-harmful content to digital services for their 'voluntary' consideration - poses significant rule of law concerns. It also undermines the authority of the EU and its Member States to advocate for better human rights standards in other jurisdictions.

Beyond content takedown, there should be clear transparency into law enforcement authorities' approach to dealing with the substantive issues arising from illegal content and illegal online activity. Too often, efforts to improve online safety slip into an 'out of sight, out of mind' mentality, whereby the overarching government and law enforcement authority objective is to remove illegal content and activity from the internet as an end

in itself. We owe to victims of illegal online activity and the public interest at large for governments and law enforcement authorities to be transparent as to the efforts they are making to address 'offline' activities that underpin online content.

10 What would be, in your view, appropriate and proportionate measures for online platforms to take in relation to activities or content which might cause harm but are not necessarily illegal?

5000 character(s) maximum

Today, the EU's approach to platform regulation focuses almost exclusively on defining platforms' obligations with respect to content as such, particularly through removal deadlines; targets for how much content should be removed; or mandates to filter certain types of content.

This 'content-centric' approach - while problematic in its own right, is wholly inappropriate for achieving regulatory goals with respect to harmful-but-legal content. Harmful-but-legal content is, by definition, legal, and the 'harmful' nature of such content can only be ascertained with reference to complex contextual factors (e.g who is consuming it; the intended meaning of the expression; historical, cultural, and social factors that inform its understanding; etc). As such, any efforts to control or suppress harmful content that borrow from the EU's existing approach to addressing illegal content (e.g. removal deadlines; filtering mandates; etc) will disproportionately interfere with individuals' freedom of expression and their due process rights. Simply put, if the Commission's objective is to address harmful content, it needs to think beyond the current 'content-centric' paradigm.

To avoid this problem, regulatory intervention should take its object to be the management of platform behaviour vis-à-vis harmful-but-legal content on their services, and not the content itself. This means - as per our answer in question one above - adopting a regulatory framework that incentives procedural accountability, whereby policy measures focus on improving platforms' trust and safety processes and procedures. We believe that firms know the most about the content-related challenges they face and are best placed to define the measures to address those challenges. In that context, the DSA should take the form of a policy framework, that provides companies with the guardrails and impetus to define the compliance measures and terms of service that reflect their specific context.

To take the example of harmful-but-legal content in algorithmic recommender systems, the DSA could include a principle-based rule of the form 'firms must take reasonable, proportionate, and feasible measures to address the virality of content that violates their defined terms-of-service'. This approach would incentivise firms to incorporate procedural accountability into how they design and operate their content recommender systems. For instance, platforms could define and implement policies that aim at minimising the amplification of certain harmful-but-legal content, or at least minimise its micro-targeting to users for whom it may be expected to give rise to harm. We can already see some nascent examples of this approach in the market, including YouTube's policies with respect to the treatment of 'borderline' content and Twitter's recent policy initiative to bring more authoritative context to the misleading tweets by public figures on the platform.

Crucially the framework of procedural accountability allows for concrete policy interventions to address the harm in harmful content, without giving rise to the fundamental rights and compliance challenges that a 'content-centric' approach to regulation entails.

11 In particular, are there specific measures you would find appropriate and proportionate for online platforms to take in relation to potentially harmful activities or content concerning minors? Please explain.

5000 character(s) maximum

We do not have recommendations for specific measures that platforms should take to address potential harmful activities or content concerning minors.

As a general rule, content responsibility should be defined in terms of principles whose application adjusts depending on the scale, risk-profile or function of a service, rather than one-size-fits-all perspective measures. The role of the DSA should be to provide the regulatory framework that incentivises these compliance measures, as per our answers in questions 1 and 10. Naturally, minors are a high-risk and vulnerable user-group, and so platforms who expressly target minors should undertake commensurate trust & safety efforts.

12 Please rate the necessity of the following measures for addressing the spread of disinformation online. Please rate from 1 (not at all necessary) to 5 (essential) each option below.

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer
Transparently inform consumers about political advertising and sponsored content, in particular during election periods	○	○	○	○	◉	○
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with user complaints	○	○	○	○	◉	○
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying false or misleading narratives	○	○	○	○	◉	○
Transparency tools and secure access to platform data for trusted researchers in order to monitor inappropriate behaviour and better understand the impact of disinformation and the policies designed to counter it	○	○	○	○	○	○
Transparency tools and secure access to platform data for authorities in order to monitor inappropriate behaviour and better understand the	○	◉	○	○	○	○

impact of disinformation and the policies designed to counter it						
Adapted risk assessments and mitigation strategies undertaken by online platforms	○	○	◉	○	○	○
Ensure effective access and visibility of a variety of authentic and professional journalistic sources	○	○	◉	○	○	○
Auditing systems for platform actions and risk assessments	○	○	○	○	◉	○
Regulatory oversight and auditing competence over platforms' actions and risk assessments, including on sufficient resources and staff, and responsible examination of metrics and capacities related to fake accounts and their impact on the manipulation and amplification of disinformation.	○	○	○	◉	○	○
Other (please specify)	○	○	○	○	○	○

13 Please specify

3000 character(s) maximum

One methodology for increasing platform transparency with respect to disinformation would be a framework whereby platforms that operate advertising networks publicly disclose all advertisements on their platforms via ad archive APIs.

If this approach was pursued, it could:
- Apply to all advertising, so as not to be constrained by arbitrary boundary definitions of 'political' or 'issue-based' advertising;
- Potentially include disclosure obligations that concern advertisers' targeting parameters for protected classes as well as aggregate audience demographics, where this makes sense given privacy and other considerations;
- Establish disclosure via publicly-available APIs, such that access is not restricted to specific privileged stakeholders as we have seen in some existing ads transparency efforts.

Previous regulatory and co-regulatory initiatives aiming at ad transparency to combat disinformation have generally focused on 'political' advertising. Focusing on purely 'political' advertising (e.g. advertising copy developed by political parties) is too narrow an approach in many instances, and is often considered to be insufficient to capture the complex web of actors involved in politically-motivated disinformation online. Moreover, a broad ads disclosure framework could also drive transparency with respect to what is known as 'issue' advertising. Experience has shown how disclosure obligations that include this broader category of political ads put platforms in a challenging position, as the relevance for disclosure purposes of particular issue-based advertising requires platforms to decide what is 'political' in nature, which can vary depending on context, jurisdiction, and time. A focus on all ads would negate this line-drawing challenge.

Further, the inclusion of all ads allows for the identification and analysis of other forms of systemic harm that

may be occurring in the current ad ecosystem. Indeed, other types of advertising that are not overtly political in nature may nonetheless be deceptive or may be targeted in a way that discriminates towards particular groups. For example, advertisements for jobs or housing may be targeted to certain demographic groups, in violation of fundamental rights.

A thoughtful analysis of how to balance privacy considerations, business considerations, and transparency is necessary for a successful transparency landscape. The inclusion of targeting parameters and aggregate audience demographics can be a significant tool for ensuring that regulators and researchers can understand how disinformation can spread across platforms. For instance, for much of the disinformation that is delivered via advertising on platforms, the content of the advertising provides only a partial - and indeed ancillary - insight into the phenomenon. Rather, it is the fact of what types of individuals those advertisements are aimed at and under what circumstances, that can provide insight into the risks and harms.

14 In special cases, where crises emerge and involve systemic threats to society, such as a health pandemic, and fast-spread of illegal and harmful activities online, what are, in your view, the appropriate cooperation mechanisms between digital services and authorities?

3000 character(s) maximum

Each crisis is unique and those that pose systemic threats to society usually require original and novel solutions and means of collaboration by various stakeholders. As such, we would caution against efforts to implement formal and rigid structures for public-private collaborations for such eventualities.

15 What would be effective measures service providers should take, in your view, for protecting the freedom of expression of their users? Please rate from 1 (not at all necessary) to 5 (essential).

	1 (not at all necessary)	2	3 (neutral)	4	5 (essential)	I don't know / No answer
High standards of transparency on their terms of service and removal decisions	○	○	○	○	◉	○
Diligence in assessing the content notified to them for removal or blocking	○	○	○	○	◉	○
Maintaining an effective complaint and redress mechanism	○	○	○	○	◉	○
Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended	○	○	○	○	◉	○
High accuracy and diligent control mechanisms, including human						

oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts	○	○	○	○	◉	○
Enabling third party insight – e.g. by academics – of main content moderation systems	○	○	○	○	◉	○
Other. Please specify	○	○	○	○	○	○

16 Please explain.

3000 character(s) maximum

A primary motivation underpinning our recommendations for the EU to focus on procedural accountability and a sliding scale or responsibility is the fact that these strategies are likely to pose less risks to individuals' freedom of expression than the alternative 'content-centric' approach. Indeed, our approach is content-agnostic in that it places the regulatory focus on platforms' processes and practices rather than mandating measures and targets with respect to third-party content. Placing the regulatory focus on the content rather than the platforms' processes is the logic that gives rise to unworkable one-hour takedown deadlines and broad upload-filtering mandates

17 Are there other concerns and mechanisms to address risks to other fundamental rights such as freedom of assembly, non-discrimination, gender equality, freedom to conduct a business, or rights of the child? How could these be addressed?

5000 character(s) maximum

Nothing specific to recommend beyond the above.

18 In your view, what information should online platforms make available in relation to their policy and measures taken with regard to content and goods offered by their users? Please elaborate, with regard to the identification of illegal content and goods, removal, blocking or demotion of content or goods offered, complaints mechanisms and reinstatement, the format and frequency of such information, and who can access the information.

5000 character(s) maximum

At a minimum, platforms should publish clear and understandable terms-of-service, that enable users to understand what behaviours and content is likely to be incompatible with the rules of the service, and what sanctions they may expect should they fail to adhere to the rules.

Services that deploy automated content control solutions (e.g. upload filters) should ensure user-facing transparency regarding the fact of these features and their goals. Likewise, services that deploy sophisticated content curation measures as a component of their trust & safety program (e.g demonetisation; down- and non-ranking; etc) should provide transparency as to the fact of these practices and their objective. Furthermore in all instances where platforms are engaged in content moderation or trust & safety-focused

curation, they should provide notice to users who are directly affected and clear and accessible means for individuals to contest decisions.

Finally, many platforms today publish transparency reports that cover online content moderation efforts. This is a welcome practice, and the Commission should encourage other entities to voluntarily publish transparency reports. However, transparency reporting often falls short when it comes to providing insight into how platforms curate content for trust & safety purposes (e.g. demonetisation; down- and non-ranking; etc). Insight into these practices and how they are deployed vis-à-vis service users is an essential means of ensuring more accountability and fundamental rights protection. Reporting exclusively on content takedowns and account suspensions is necessary but sometimes not sufficient.

19 What type of information should be shared with users and/or competent authorities and other third parties such as trusted researchers with regard to the use of automated systems used by online platforms to detect, remove and/or block illegal content, goods, or user accounts?

5000 character(s) maximum

Trusted researchers and government officials should - subject to adherence to data protection, intellectual property, and trade secrets law - be empowered to scrutinise the workings of certain automated content control systems to assess their impact on fundamental rights and the risk of output discrimination, as part of a broader framework of algorithmic oversight.

Beyond disclosure, companies should be encouraged to keep documentation as to how their automated trust and safety systems work; the objective and goals of those systems; the degree of human oversight; the systems' effectiveness; and the recurring procedures the companies have implemented to detect and address system failure.

While not related to automated content control, we would like to nonetheless provide recommendations with respect to advertising disclosure (as articulated in our response to question 12 and our responses in section V). Disclosure of this kind should be broader than with respect to algorithmic content control or recommender systems, and should be operationalised via publicly-available APIs. It is feasible to adopt a broader approach therein as the disclosure framework we envisage - focused around advertising content and targeting parameters - is compatible with data protection law and so there is no need for specific restrictions on access.

That kind of public-facing transparency can enable diffused multi-level oversight and engender a culture of 'permissionless transparency' with regard to the research into disinformation on platforms. Governments alone may lack the expertise or capacity to undertake all of the required research. Moreover, restricting access to privileged researchers creates boundary and selection challenges, and increases the risk that certain critical research questions or monitoring activities (particularly in relation to oppressed and vulnerable groups) will be underserved.

20 In your view, what measures are necessary with regard to algorithmic recommender systems used by online platforms?

5000 character(s) maximum

There are a number of different types of recommender systems. Of the various types, 'open' recommender systems are the most relevant for discussions around illegal and harmful content. These types of

recommender systems select, rank, present, and ultimately amplify third-party content prior moderation.

When platforms make specific interventions to amplify third-party content through these systems, they should reasonably be expected to make greater efforts to ensure that content is not illegal or likely to cause harm. In that respect recommender systems are an important case-in-point as to why the DSA should be built around a principle of procedural accountability. The harmful outcomes that arise from recommender systems are influenced by the platforms' business practices and processes - what they are choosing to amplify, to whom and how. To minimise those harmful outcomes, policy interventions should thus aim at ensuring that platforms 'recommend better'. Simply forcing platforms to remove more content in ever shorter periods of time will not address this problem, and on the contrary, will engender worse outcomes.

Unfortunately our ability to define what policy interventions could improve 'open' recommender systems is impeded by a systemic lack of insight into how they work and the types of negative social outcomes that they may be engendering. In that context, the European Commission should first focus on bringing more transparency to the recommending ecosystem.

In that context, the Commission should consider measures that ensure researchers and relevant oversight authorities have insight into what a recommender system is designed to achieve (e.g. to maximise engagement with content) and the conceptual means by which it achieves that (e.g. by microtargeting content that specific users are likely to find relevant and interesting). Understanding what a system is designed to do is a prerequisite for understanding how to ensure that system works properly. This granular insight should be complemented by a greater focus on transparency of curative processes vis-à-vis users (e.g. 'why am I seeing this' product features should provide meaningful and personalised insight to the requesting user).

We would also encourage the Commission to consider how greater transparency could be engendered with respect to what content is being recommended and the targeting parameters associated with it. Any disclosure of the kind should be aggregated in nature so as not to reveal insights into particular users. Data about the recommendations - whether the system is recommending cooking classes or white supremacists videos - will provide the most direct insight into potential harm and into whether a company is satisfying its procedural responsibilities.

In addition, the Commission should consider whether the code for recommendation systems should be publicly available or, at a minimum, available for inspection by regulators under certain legal processes. Such an approach needs to be considered with care, as it would risk divulging a company's trade secrets but comes with the benefit of ensuring these systems can be more broadly audited, so that we are not left to simply trust that companies are optimising for quality over engagement.

21 In your view, is there a need for enhanced data sharing between online platforms and authorities, within the boundaries set by the General Data Protection Regulation? Please select the appropriate situations, in your view:

- [ ] For supervisory purposes concerning professional users of the platform - e.g. in the context of platform intermediated services such as accommodation or ride-hailing services, for the purpose of labour inspection, for the purpose of collecting tax or social security contributions
- [x] For supervisory purposes of the platforms' own obligations – e.g. with regard to content moderation obligations, transparency requirements, actions taken

in electoral contexts and against inauthentic behaviour and foreign interference

- [ ] Specific request of law enforcement authority or the judiciary
- [ ] On a voluntary and/or contractual basis in the public interest or for other purposes

22 Please explain. What would be the benefits? What would be concerns for companies, consumers or other third parties?

5000 character(s) maximum

See our response to question 12 and question 19 concerning the disclosure of all advertising on platforms.

23 What types of sanctions would be effective, dissuasive and proportionate for online platforms which systematically fail to comply with their obligations (See also the last module of the consultation)?

5000 character(s) maximum

Given the complex nature of the regulatory regime and the extent to which breaches can differ in terms of severity and fault, it is prudent for the Commission to pursue a graduated approach to enforcement.

Ultimately, the regulatory objective should be to ensure and optimise compliance with the rules, rather than simply punish rule-breakers for the sake of it. The most effective means of ensuring compliance is to empower firms to define and implement the specific measures and procedures most appropriate for achieving the regulatory objectives. The regulator's role should first and foremost be to oversee and check that these efforts are meeting the regulatory objectives, and if not, to provide guidance and recommendations for improvement. This approach to enforcement is likely to provide the least cost to the regulator, and more importantly, engender the kind of trusted relationship and culture of accountability that the DSA regime aims at.

Coercive measures should only be considered where companies are systematically and intentionally ignoring regulatory objectives. Coercive measures themselves should be graduated in nature, and could range from 'naming and shaming' to monetary fines for the most egregious breaches of company behaviour.

Ultimately, new enforcement structures under the DSA should be without prejudice to the intermediary liability provisions of the E-Commerce directive and the established safe harbours that they afford.

24 Are there other points you would like to raise?

3000 character(s) maximum

II. Reviewing the liability regime of digital services acting as intermediaries?

The liability of online intermediaries is a particularly important area of internet law in Europe and worldwide. The E-Commerce Directive harmonises the liability exemptions applicable to online intermediaries in the

single market, with specific provisions for different services according to their role: from Internet access providers and messaging services to hosting service providers.
The previous section of the consultation explored obligations and responsibilities which online platforms and other services can be expected to take – i.e. processes they should put in place to address illegal activities which might be conducted by users abusing their service. In this section, the focus is on the legal architecture for the liability regime for service providers when it comes to illegal activities conducted by their users. The Commission seeks informed views on hos the current liability exemption regime is working and the areas where an update might be necessary.

2 The liability regime for online intermediaries is primarily established in the E-Commerce Directive, which distinguishes between different types of services: so called ‘mere conduits’, ‘caching services’, and ‘hosting services’.
In your understanding, are these categories sufficiently clear and complete for characterising and regulating today’s digital intermediary services? Please explain.

5000 character(s) maximum

The categories of ‘mere conduits’ and ‘caching services’ are sufficiently clear, and we do not see a need to amend them. That said, owing to commercial and technological developments, the distinct category of ‘caching’ is arguably less relevant today than it was at the time of the E-Commerce directive's drafting.

The situation with respect to the ‘hosting services’ category is more complex. The innovation-friendly environment that was facilitated by the E-Commerce directive has contributed to the development of a variety of new services and business models over the last twenty years. Given that many of these services depend on the hosting of third-party content, they have tended to be viewed within the E-Commerce directive’ s ‘hosting services’ category. The broad nature of the ‘hosting services’ category has thus ensured that new and innovative online services can grow without fear of crippling liability risk.

However, problems arise because the EU and its Member States have tended to use the intermediary categories of the E-Commerce directive and the corresponding liability provisions as a vector for content regulation. Typically, this has manifested in regulations that make eligibility for intermediary liability protection contingent on the implementation of certain measures by the intermediary (e.g. deploying upload filters). Given that so many different types of services fall under the scope of article 14, regulations that tighten the eligibility criteria for safe harbour protection (even if ostensibly aimed at a set few companies or business models) can have wide-ranging collateral impact.

The broad nature of the E-Commerce directive intermediary categories (particularly article 14) is one of its greatest strengths. We do not see a reason to review the categories or amend them. However, we would strongly encourage the Commission to decouple its content regulation efforts from the provisions of the E-Commerce directive. As noted above, the contemporary approach tends to give rise to blunt one-size-fits-all regulation, and catastrophic risk for companies who struggle to meet the increasingly-strict criteria for safe harbour eligibility.

As we explain in section I.II in this consultation, the Commission can achieve its content regulation objectives while maintaining the key principles of the E-Commerce directive by implementing a complementary procedural accountability framework for certain digital service providers.

For hosting services, the liability exemption for third parties' content or activities is conditioned by a knowledge standard (i.e. when they get 'actual knowledge' of the illegal activities, they must 'act expeditiously' to remove it, otherwise they could be found liable).

3 Are there aspects that require further legal clarification?

5000 character(s) maximum

We noted above that in recent years the EU and Member States legislators, as well as EU-level and national-level courts, have attempted to clarify the meaning of the E-Commerce Directive's 'hosting services' category to advance their content regulation objectives.

One such example of this phenomenon is the so-called 'active versus passive' hosting distinction, whereby service providers normally eligible for article 14 safe harbour are deemed to lose that protection in the event that they are 'active' with respect to the third-party content on their services. While we agree that under EU law the hosting safe harbour must have a boundary related to a firm's activity, the 'active-passive' distinction as some EU court rulings have defined it in the past have implicated far too broad a class of intermediaries. It implicitly characterises many rudimentary, reasonable, and trivial curative actions of hosting service providers as being impermissible if that service wishes to maintain its safe harbour protections.

In that context, we encourage the European Commission to capitalise on the DSA initiative as an opportunity to clarify the 'active-versus-passive' phenomenon within the EU regulatory landscape. The DSA should provide clarity that services that engage in the ordinary kinds of curative measures are not at risk of liability for doing so. The degree of 'activity' that would take an entity outside the remit of article 14 protection should be far more narrowly scoped and reserved for only the most intensive practices, as was originally intended in the E-Commerce directive.

4 Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected.

5000 character(s) maximum

It is well-known that the E-Commerce directive does not contain a 'good samaritan' clause to shield intermediaries from liability for good-faith content moderation efforts. We do not have a specific perspective on whether the lack of such a shield means intermediaries are disincentivised from taking proactive measures. The fact that many intermediaries today do take voluntary measures would suggest that, at least in practice, there is not a major disincentive.

In any case, should the European Commission proceed with new regulatory interventions that oblige digital service providers to undertake greater content moderation or procedural measures, it will be important to clarify that such efforts will not compromise the delicate balance struck in the E-Commerce Directive intermediary liability provisions. As noted above, an obvious step to that end would be to clarify the 'active-versus-passive' hosting distinction to mitigate problematic interpretations of recital 42 of the E-Commerce directive.

5 Do you think that the concept characterising intermediary service providers as playing a role of a 'mere technical, automatic and passive nature' in the

transmission of information (recital 42 of the E-Commerce Directive) is sufficiently clear and still valid? Please explain.

5000 character(s) maximum

The concept remains sufficiently clear and valid with respect to 'mere conduit' and 'caching' activities. However, as we note in our response to question 3, the concept has been interpreted in problematic ways with respect to 'hosting service providers'.

In the context of hosting, this concept has given rise to the binary 'active versus passive' distinction. The binary interpretation has created a situation where hosting service providers are at risk of losing safe harbour eligibility when they engage in rudimentary, trivial, and reasonable practices related to the content that they host.

It is evident that the concept of recital 42 is not flexible enough to take into account the considerable innovation in technologies and business models that have occurred at the hosting layer in the last 20 years. In that context, we recommend the Commission to use the DSA as an opportunity to revisit this concept and clarify a much-narrower scope to 'active' hosting.

6 The E-commerce Directive also prohibits Member States from imposing on intermediary service providers general monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users. In your view, is this approach, balancing risks to different rights and policy objectives, still appropriate today? Is there further clarity needed as to the parameters for 'general monitoring obligations'? Please explain.

5000 character(s) maximum

As a principle, the 'no general monitoring' provision of article 15 of the E-Commerce directive remains an essential bulwark against fundamental rights breaches and disproportionate compliance burdens in the online ecosystem. Simply put, without a prohibition on general monitoring, legislators and courts could force intermediaries to monitor the activity of large swathes or all of their users' activity, constituting an acute interference with the rights to privacy and data protection; freedom of expression; and the freedom to conduct a business, as enshrined in the EU Charter of Fundamental Rights. These considerations are as pertinent today as they were when the E-Commerce directive was implemented.

Yet the unelaborated nature of article 15 of the E-Commerce directive has contributed to fragmented and problematic interpretations of what the prohibition on general monitoring means by legislators and courts (e. g. article 17 of the directive on copyright in the digital single market; Glawischnig-Piesczek v. Facebook Ireland Limited). Evidently, it is difficult to prescribe the contours of 'general' and 'specific' monitoring in abstract terms, given the heterogeneity of online business models and monitoring use-cases. For instance, a court could consider that an injunction that directs a social media platform to prevent the reappearance of a certain piece of content might constitute 'specific' monitoring, but when said platform has billions of users, and technical enforcement of the injunction requires content scanning for every posting by each of those users, it is hard to consider such a monitoring mandate as not being 'general'.

In that context, there would likely be merit in the European Commission providing guidance or clarity as to the criteria courts and legislators should consider when making assessments as to the meaning of Article 15,

and whether certain monitoring mandates are admissible. Such guidance should build on the case law of the CJEU SABAM versus Scarlett Extended and Netlog versus SABAM, and elaborate on the risks that general monitoring measures can have on fundamental rights.

7 Do you see any other points where an upgrade may be needed for the liability regime of digital services acting as intermediaries?

5000 character(s) maximum

We do not believe that any upgrade is required for the EU's intermediary liability regime, notwithstanding the need to clarify the 'active versus passive' distinction.

The regime remains incredibly important for start-ups, scale-ups, and challenger companies, and to weaken it would simply cement the power of a handful of large market actors without bringing any discernible benefit.

We note that much of the pressure to reform the intermediary liability provisions of the E-Commerce directive arise from a belief that those provisions are a barrier to meaningful content responsibility on the part of digital services. As we outline in our responses in section I.II, it is feasible for the EU to pursue its content regulation objectives in a manner which is protective of fundamental rights, digital competition, and which does not require sacrificing the crucial benefits of the E-Commerce directive.

III. What issues derive from the gatekeeper power of digital platforms?

There is wide consensus concerning the benefits for consumers and innovation, and a wide-range of efficiencies, brought about by online platforms in the European Union's Single Market. Online platforms facilitate cross-border trading within and outside the EU and open entirely new business opportunities to a variety of European businesses and traders by facilitating their expansion and access to new markets. At the same time, regulators and experts around the world consider that large online platforms are able to control increasingly important online platform ecosystems in the digital economy. Such large online platforms connect many businesses and consumers. In turn, this enables them to leverage their advantages – economies of scale, network effects and important data assets- in one area of their activity to improve or develop new services in adjacent areas. The concentration of economic power in then platform economy creates a small number of 'winner-takes it all/most' online platforms. The winner online platforms can also readily take over (potential) competitors and it is very difficult for an existing competitor or potential new entrant to overcome the winner's competitive edge.
The Commission announced that it 'will further explore, in the context of the Digital Services Act package, ex ante rules to ensure that markets characterised by large platforms with significant network effects acting as gatekeepers, remain fair and contestable for innovators, businesses, and new market entrants'.
This module of the consultation seeks informed views from all stakeholders on this framing, on the scope, the specific perceived problems, and the implications, definition and parameters for addressing possible issues deriving from the economic power of large, gatekeeper platforms.
The Communication 'Shaping Europe's Digital Future' also flagged that 'competition policy alone cannot address all the systemic problems that may arise in the platform economy'. Stakeholders are invited to provide their views on potential new competition instruments through a separate, dedicated open public consultation that will be launched soon.
In parallel, the Commission is also engaged in a process of reviewing EU competition rules and ensuring they are fit for the modern economy and the digital age. As part of that process, the Commission has launched a consultation on the proposal for a New Competition Tool aimed at addressing the gaps

identified in enforcing competition rules. The initiative intends to address as specific objectives the structural competition problems that prevent markets from functioning properly and that can tilt the level playing field in favour of only a few market players. This could cover certain digital or digitally-enabled markets, as identified in the report by the Special Advisers and other recent reports on the role of competition policy, and/or other sectors. As such, the work on a proposed new competition tool and the initiative at stake complement each other. The work on the two impact assessments will be conducted in parallel in order to ensure a coherent outcome. In this context, the Commission will take into consideration the feedback received from both consultations. We would therefore invite you, in preparing your responses to the questions below, to also consider your response to the parallel consultation on a new competition tool .

1 To what extent do you agree with the following statements?

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/ No reply
Consumers have sufficient choices and alternatives to the offerings from online platforms.	○	○	○	○	○	○
It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by other online platform companies (“multi-home”).	○	○	○	○	○	○
It is easy for individuals to port their data in a useful manner to alternative service providers outside of an online platform.	○	○	○	○	○	○
There is sufficient level of interoperability between services of different online platform companies.	○	○	○	○	○	○
There is an asymmetry of information between the knowledge of online platforms about consumers, which enables them to target them with commercial offers, and the knowledge of consumers about market conditions.	○	○	○	○	○	○

It is easy for innovative SME online platforms to expand or enter the market.						
Traditional businesses are increasingly dependent on a limited number of very large online platforms.						
There are imbalances in the bargaining power between these online platforms and their business users.						
Businesses and consumers interacting with these online platforms are often asked to accept unfavourable conditions and clauses in the terms of use/contract with the online platforms.						
Certain large online platform companies create barriers to entry and expansion in the Single Market (gatekeepers).						
Large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital) to expand into other activities.						
When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from smaller innovative market operators.						

Main features of gatekeeper online platform companies and the main criteria for assessing their economic power

1 Which characteristics are relevant in determining the gatekeeper role of large online platform companies? Please rate each criterion identified below from 1 (not relevant) to 5 (very relevant):

Large user base	
Wide geographic coverage in the EU	
They capture a large share of total revenue of the market you are active/of a sector	
Impact on a certain sector	
They build on and exploit strong network effects	
They leverage their assets for entering new areas of activity	
They raise barriers to entry for competitors	
They accumulate valuable and diverse data and information	
There are very few, if any, alternative services available on the market	
Lock-in of users/consumers	
Other	

2 If you replied "other", please list

3000 character(s) maximum

All of the factors identified above could potentially impact what constitutes a gatekeeping function, depending on the circumstances. A better internet necessarily needs room for new, small or medium, and independent players to provide innovative solutions that benefit consumers in ways that major platforms cannot provide.

From our own experience, online platform companies at various levels of the internet stack provide us with

important opportunities to offer innovative services and meet European consumers where they are. In some instances, we are dependent on certain types of platforms in order to reach consumers (e.g. operating systems).

While this dependency is not in itself a problem (and indeed, ensures we have access to many more consumers), it does mean that we are vulnerable to 'upstream' decisions by the platform provider that might have negative 'downstream' implications, and have limited ability to impact the upstream world given the size and nature of our product and organisation.

In that context, while we do not have a specific definition in mind for 'gatekeeper' platforms, we would encourage the European Commission to take into account vertical market dependencies when considering definitions.

3 Please explain your answer. How could different criteria be combined to accurately identify large online platform companies with gatekeeper role?

3000 character(s) maximum

We do not have specific considerations as to how different criteria could be combined in order to accurately identify gatekeeping platforms. Rather, we simply consider situations defined by vertical market dependencies as being relevant for any cumulative definition of gatekeeping.

4 Do you believe that the integration of any or all of the following activities within a single company can strengthen the gatekeeper role of large online platform companies ('conglomerate effect')? Please select the activities you consider to steengthen the gatekeeper role:

- [x] online intermediation services (i.e. consumer-facing online platforms such as e-commerce marketplaces, social media, mobile app stores, etc., as per Regulation (EU) 2019/1150 - see glossary)
- [ ] search engines
- [x] operating systems for smart devices
- [ ] consumer reviews on large online platforms
- [ ] network and/or data infrastructure/cloud services
- [ ] digital identity services
- [x] payment services (or other financial services)
- [ ] physical logistics such as product fulfilment services
- [ ] data management platforms
- [ ] online advertising intermediation services
- [ ] other. Please specify in the text box below.

5 Other - please list

1000 character(s) maximum

Emerging issues

The following questions are targeted particularly at businesses and business users of large online platform companies.

2 As a business user of large online platforms, do you encounter issues concerning trading conditions on large online platform companies?

- (●) Yes
- ( ) No

3 Please specify which issues you encounter and please explain to what types of platform these are related to (e.g. e-commerce marketplaces, app stores, search engines, operating systems, social networks).

5000 character(s) maximum

As a client application, we depend on operating systems and application store providers in order to reach European consumers. These intermediaries have provided an unprecedented basis on which we can grow our products and reach consumers where they are.

These relationships are often symbiotic - we benefit from greater access to new users and operating system /application stores make their platforms more attractive by offering the third-party services like Firefox that their customers may want to use.

However, the dependence we have on these platforms can often make us vulnerable to 'upstream' decisions that have 'downstream' consequences. This can occur where an upstream decision fails to adequately take into account the impact on small, medium, or independent players in an ecosystem, which could be the result of lack of awareness, lack of prioritisation of downstream players, or competing corporate interests not intending to cause competitive harm. This could also occur in situations where the platform has a product that competes directly, and undertakes intentional or unintentional actions that have negative consequences for our ability to compete. In both of these instances, consumers are often the ones who ultimately lose out - either because they lose the opportunity to try an alternative solution, or because the upstream decisions limit the ability of small or independent players to provide a competitive offering in the market and enable users to have a competitive choice for services.

As we explain in our response to question four, some of our experiences fall within the description above, where upstream decisions have problematic consequences in our dependent market.

4 Have you been affected by unfair contractual terms or unfair practices of very large online platform companies? Please explain your answer in detail, pointing to the effects on your business, your consumers and possibly other stakeholders in the short, medium and long-term?

5000 character(s) maximum

Operating systems and app stores provide us with a crucial means of serving our customers. There are certain practices that, if undertaken by these platforms, can ensure that a healthy and open ecosystem is maintained. In many instances, we see decisions that enable a flourishing online ecosystem.

For instance, products like Firefox can thrive when operating systems and app store providers allow users to change their default browser, preferably in an efficient way and where preferences are honoured through time. In addition, we believe that consumer welfare is optimised when consumers have different products to choose from. For that reason, we welcome the efforts by platforms like Android to ensure openness, by allowing third-party browsers access into the application ecosystem on reasonable terms.

Firefox serves as a window to the web, and like other vendors, we invest heavily in optimising the web experience and providing innovative features for consumers. We also do our utmost to communicate our product features and differentiation to consumers, taking advantage of whatever channels are at our disposal. However, as we do not control operating systems or app stores, we do not benefit from some of the most important channels for influencing consumer preferences.

For instance, an operating system can send notifications and prompts to device users to promote its browser product in a way that a third-party browser cannot. While leveraging products and assets in this way is often logical and reasonable, we encourage operating system and app store providers to use that capacity prudently.

For our own competitive experience, as well as for other similarly situated providers of online services, we encourage the major platforms to consider the downstream impacts of cross-promotion or platform leverage to ensure that ecosystems can successfully thrive.

The following questions are targeted particularly at consumers who are users of large online platform companies.

6 Do you encounter issues concerning commercial terms and conditions when accessing services provided by large online platform companies?
Please specify which issues you encounter and please explain to what types of platform these are related to (e.g. e-commerce marketplaces, app stores, search engines, operating systems, social networks).

5000 character(s) maximum

7 Have you considered any of the practices by large online platform companies as unfair? Please explain.

3000 character(s) maximum

The following questions are open to all respondents.

9 Are there specific issues and unfair practices you perceive on large online platform companies?

5000 character(s) maximum

See our response to question three and question four above.

10 In your view, what practices related to the use and sharing of data in the platforms' environment are raising particular challenges?

5000 character(s) maximum

11 What impact would the identified unfair practices can have on innovation, competition and consumer choice in the single market?

3000 character(s) maximum

As we have mentioned, we depend on certain platforms like operating systems and application stores to grow our products and reach European consumers where they are. As such, these platforms offer us tremendous opportunity and they in effect serve as the basis on which new innovative markets develop.

We see our company and our products as having unique value to European consumers and the internet ecosystem more broadly. Our Firefox web browser provides European consumers with a window to the web, and ensures privacy and security are fundamental. Moreover, as a mission driven company and a Foundation we see our role as maintaining and advancing the health of the internet ecosystem. On that basis, we play a key role in internet standard-setting processes and in the deployment of new web protocols, ensuring that the web remains an open ecosystem. Having successful monetisable products allows us to continue that important work.

Our ultimate desire then is simply to be able to compete on the merits and provide European consumers with meaningful choice. It is important for both the browser market and the broader internet ecosystem that companies like Mozilla exist and thrive. Services like those offered by Mozilla drive innovation, create new technologies that help contribute to upleveling of entire markets on consumer friendly practices (such as has been born out with enhanced tracking protection, now widely adopted across the browser industry), and help protect the internet as a dynamic and adaptable place, with the low barriers to entry for new ideas and players.

12 Do startups or scaleups depend on large online platform companies to access or expand? Do you observe any trend as regards the level of dependency in the last five years (i.e. increases; remains the same; decreases)? Which difficulties in your view do start-ups or scale-ups face when they depend on large online platform companies to access or expand on the markets?

3000 character(s) maximum

13 Which are possible positive and negative societal (e.g. on freedom of expression, consumer protection, media plurality) and economic (e.g. on market contestability, innovation) effects, if any, of the gatekeeper role that large online platform companies exercise over whole platform ecosystem?

3000 character(s) maximum

We have noted at various points that as an independent client application, products like the Firefox web browser depend on operating systems and application store providers in order to reach European consumers. These intermediaries have provided an unprecedented basis on which we can grow our products and reach consumers where they are.

Relationships between large platforms and downstream market participants are often symbiotic. In our market case, large platforms can provide us with greater access to new users, and operating system /application stores make their platforms more attractive by offering the third-party services like Firefox that their customers may want to use. In these situations, 'gatekeeping' platforms can serve as important enablers of freedom of expression, consumer choice, and downstream innovation.

However, relationships between major platforms and participants in downstream markets are not always fully balanced. Where distortions are particularly acute, this can give rise to less consumer choice and the inability of independent companies to develop innovative new products.

Ultimately, we believe that a healthy internet ecosystem is an open internet ecosystem. Openness and contestable markets will ensure European consumers can enjoy the full benefit of the internet, in terms of the innovative product offerings that it can provide, and the enabling role it can play for individuals' freedom of expression.

14 Which issues specific to the media sector (if any) would, in your view, need to be addressed in light of the gatekeeper role of large online platforms? If available, please provide additional references, data and facts.

3000 character(s) maximum

Regulation of large online platform companies acting as gatekeepers

1 Do you believe that in order to address any negative societal and economic effects of the gatekeeper role that large online platform companies exercise over whole platform ecosystems, there is a need to consider dedicated regulatory rules?

- ☐ I fully agree
- ☑ I agree to a certain extent
- ☐ I disagree to a certain extent
- ☐ I disagree
- ☐ I don't know

2 Please explain

3000 character(s) maximum

As an initial matter, we recognise the tremendous complexity that the Commission faces in navigating these challenges, to ensure that the regulatory regimes implemented have a net positive impact on consumers and help build a better internet across the European Union's single market and beyond. We believe that, as a matter of policy, that the consideration of dedicated regulatory rules is an important component of a digital strategy overall.

In particular, we encourage the Commission to consider ways that consumers could be protected, and the playing field leveled for competitors, in situations where gatekeeping platforms hold tremendous upstream power, or otherwise control a vertically integrated system where independent competitors at various points in the ecosystem must overcome the competitive advantages of the major players in order to compete and thrive.

3 Do you believe that such dedicated rules should prohibit certain practices by large online platform companies with gatekeeper role that are considered particularly harmful for users and consumers of these large online platforms?

- (●) Yes
- ( ) No
- ( ) I don't know

4 Please explain your reply and, if possible, detail the types of prohibitions that should in your view be part of the regulatory toolbox.

3000 character(s) maximum

While any new regulatory regime must carefully consider the potential harms as well as the potential benefits of the rules it considers propagating, as an initial matter, rules that respect consumer selections may be potentially net positive across the ecosystem. One example of a place where such prohibitions could benefit consumers and enable a healthy market would be rules around how major players can cross-promote products fairly and thoughtfully. Another example where the potential benefit could be net positive would be around enabling consumers to override defaults and set meaningful choices that are not undermined by the vertically integrated platform.

5 Do you believe that such dedicated rules should include obligations on large online platform companies with gatekeeper role?

- (●) Yes
- ( ) No
- ( ) I don't know

6 Please explain your reply and, if possible, detail the types of obligations that should in your view be part of the regulatory toolbox.

3000 character(s) maximum

We believe that policy should aim to ensure respect for consumer choice, as per our response to question 4

7 If you consider that there is a need for such dedicated rules setting prohibitions and obligations, as those referred to in your replies to questions 3 and 5 above, do you think there is a need for a specific regulatory authority to enforce these rules?

- (●) Yes
- ( ) No
- ( ) I don't know

8 Please explain your reply.

3000 character(s) maximum

If there is to be a new ex ante regulatory regime, it is essential that the regime is nimble, flexible, and does not act as a barrier to innovation in the future. A regulatory authority can play a useful role in that regard, by responding to problems as they emerge and ensuring that generalised rules can be properly applied and understood in the specific market situations.

To ensure consistency of rules and of enforcement, it would be preferable for oversight to be structured at the EU level.

9 Do you believe that such dedicated rules should enable regulatory intervention against specific large online platform companies, when necessary, with a case by case adapted remedies?

- ( ) Yes
- ( ) No
- (●) I don't know

10 If yes, please explain your reply and, if possible, detail the types of case by case remedies.

3000 character(s) maximum

11 If you consider that there is a need for such dedicated rules, as referred to in question 9 above, do you think there is a need for a specific regulatory authority to enforce these rules?

- ( ) Yes
- ( ) No

12 Please explain your reply

3000 character(s) maximum

13 If you consider that there is a need for a specific regulatory authority to enforce dedicated rules referred to questions 3, 5 and 9 respectively, would in your view these rules need to be enforced by the same regulatory authority or could they be enforced by different regulatory authorities? Please explain your reply.

3000 character(s) maximum

To ensure consistency of rules and of enforcement, it would be preferable for oversight to be structured at the EU level.

14 At what level should the regulatory oversight of platforms be organised?

- At national level
- At EU level
- Both at EU and national level.
- I don't know

15 If you consider such dedicated rules necessary, what should in your view be the relationship of such rules with the existing sector specific rules and/or any future sector specific rules?

3000 character(s) maximum

16 Should such rules have an objective to tackle both negative societal and negative economic effects deriving from the gatekeeper role of these very large online platforms? Please explain your reply.

3000 character(s) maximum

If there are to be ex ante rules, those rules should focus exclusively on ensuring market contestability and addressing structural problems with how certain digital markets operate. Focusing on broader societal issues (e.g. illegal content) would likely create additional complexities and stretch regulatory capacity too thinly, as well as increase the potential for negative unintended consequences of regulatory activity on expression and innovation.

17 Specifically, what could be effective measures related to data held by very large online platform companies with a gatekeeper role beyond those laid down in the General Data Protection Regulation in order to promote competition and innovation as well as a high standard of personal data protection and consumer welfare?

3000 character(s) maximum

See our submission to the public consultation on the EU Data strategy here: https://blog.mozilla.org/netpolicy/2020/06/05/eudatastrategy/

18 What could be effective measures concerning large online platform companies with a gatekeeper role in order to promote media pluralism, while respecting the subsidiarity principle?

3000 character(s) maximum

19 Which, if any, of the following characteristics are relevant when considering the requirements for a potential regulatory authority overseeing the large online platform companies with the gatekeeper role:

- [x] Institutional cooperation with other authorities addressing related sectors – e. g. competition authorities, data protection authorities, financial services authorities, consumer protection authorities, cyber security, etc.
- [x] Pan-EU scope
- [ ] Swift and effective cross-border cooperation and assistance across Member States
- [ ] Capacity building within Member States
- [x] High level of technical capabilities including data processing, auditing capacities
- [ ] Cooperation with extra-EU jurisdictions
- [ ] Other

21 Please explain if these characteristics would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?

3000 character(s) maximum

22 Which, if any, of the following requirements and tools could facilitate regulatory oversight over very large online platform companies (multiple answers possible):

- [ ] Reporting obligation on gatekeeping platforms to send a notification to a public authority announcing its intention to expand activities
- [x] Monitoring powers for the public authority (such as regular reporting)
- [x] Investigative powers for the public authority

☐ Other

24 Please explain if these requirements would need to be different depending on the type of ex ante rules (see questions 3, 5, 9 above) that the regulatory authority would be enforcing?

3000 character(s) maximum

25 Taking into consideration the parallel consultation on a proposal for a New Competition Tool focusing on addressing structural competition problems that prevent markets from functioning properly and tilt the level playing field in favour of only a few market players. Please rate the suitability of each option below to address market issues arising in online platforms ecosystems. Please rate the policy options below from 1 (not effective) to 5 (most effective).

	1 (not effective)	2 (somewhat effective)	3 (sufficiently effective)	4 (very effective)	5 (most effective)	Not applicable /No relevant experience or knowledge
1. Current competition rules are enough to address issues raised in digital markets	○	○	○	○	○	○
2. There is a need for an additional regulatory framework imposing obligations and prohibitions that are generally applicable to all large online platforms with gatekeeper power	○	○	○	○	○	○
3. There is a need for an additional regulatory framework allowing for the possibility to impose tailored remedies on individual large online platforms with gatekeeper power, on a case-by-case basis	○	○	○	○	○	○
4. There is a need for a New Competition Tool allowing to address structural risks and lack of competition in (digital) markets on a case-by-case basis.	○	○	○	○	○	○
5. There is a need for combination of two or more of the options 2 to 4.	○	○	○	○	○	○

26 Please explain which of the options, or combination of these, would be, in your view, suitable and sufficient to address the market issues arising in the online platforms ecosystems.

3000 character(s) maximum

27 Are there other points you would like to raise?

3000 character(s) maximum

IV. Other emerging issues and opportunities, including online advertising and smart contracts

Online advertising has substantially evolved over the recent years and represents a major revenue source for many digital services, as well as other businesses present online, and opens unprecedented opportunities for content creators, publishers, etc. To a large extent, maximising revenue streams and optimising online advertising are major business incentives for the business users of the online platforms and for shaping the data policy of the platforms. At the same time, revenues from online advertising as well as increased visibility and audience reach are also a major incentive for potentially harmful intentions, e.g. in online disinformation campaigns.
Another emerging issue is linked to the conclusion of 'smart contracts' which represent an important innovation for digital and other services, but face some legal uncertainties.
This section of the open public consultation seeks to collect data, information on current practices, and informed views on potential issues emerging in the area of online advertising and smart contracts. Respondents are invited to reflect on other areas where further measures may be needed to facilitate innovation in the single market. This module does not address privacy and data protection concerns; all aspects related to data sharing and data collection are to be afforded the highest standard of personal data protection.

Online advertising

1 When you see an online ad, is it clear to you who has placed it online?

- Yes, always
- Sometimes: but I can find the information when this is not immediately clear
- Sometimes: but I cannot always find this information
- I don't know
- No

2 As a publisher online (e.g. owner of a website where ads are displayed), what types of advertising systems do you use for covering your advertising space? What is their relative importance?

	% of ad space	% of ad revenue
Intermediated programmatic advertising though real-time bidding		
Private marketplace auctions		
Programmatic advertising with guaranteed impressions (non-auction based)		
Behavioural advertising (micro-targeting)		
Contextual advertising		
Other		

3 What information is publicly available about ads displayed on an online platform that you use?

3000 character(s) maximum

4 As a publisher, what type of information do you have about the advertisement placed next to your content/on your website?

3000 character(s) maximum

5 To what extent do you find the quality and reliability of this information satisfactory for your purposes?

Please rate your level of satisfaction	

6 As an advertiser or an agency acting on behalf of the advertiser (if applicable), what types of programmatic advertising do you use to place your ads? What is their relative importance in your ad inventory?

	% of ad inventory	% of ad expenditure
Intermediated programmatic advertising though real-time bidding		
Private marketplace auctions		
Programmatic advertising with guaranteed impressions (non-auction based)		
Behavioural advertising (micro-targeting)		
Contextual advertising		
Other		

7 As an advertiser or an agency acting on behalf of the advertiser (if applicable), what type of information do you have about the ads placed online on your behalf?

3000 character(s) maximum

8 To what extent do you find the quality and reliability of this information satisfactory for your purposes?

Please rate your level of satisfaction	☆ ☆ ☆ ☆ ☆

The following questions are targeted specifically at online platforms.

10 As an online platform, what options do your users have with regards to the advertisements they are served and the grounds on which the ads are being served to them? Can users access your service through other conditions than viewing advertisements? Please explain.

3000 character(s) maximum

11 Do you publish or share with researchers, authorities or other third parties detailed data on ads published, their sponsors and viewership rates? Please explain.

3000 character(s) maximum

12 What systems do you have in place for detecting illicit offerings in the ads you intermediate?

3000 character(s) maximum

The following questions are open to all respondents.

14 Based on your experience, what actions and good practices can tackle the placement of ads next to illegal content or goods, and/or on websites that disseminate such illegal content or goods, and to remove such illegal content or goods when detected?

3000 character(s) maximum

Today the advertising ecosystem is very opaque, and it remains almost impossible for a third party to establish why and how an advertisement was ultimately placed in a specific 'space' online, let alone identify best practices for minimising concerning ad placement. As a result, it is difficult to identify particular best practices for minimising the placement of advertising alongside illegal content.

Yet beyond ad placement issues, this underlying opacity creates the conditions for a host of negative outcomes that we see today in the ecosystem. These range from ad fraud; to data leakage; to invasive data collection practices; and a general lack of trust amongst the various stakeholders in the ecosystem, be they consumers, advertisers, publishers, and ad networks.

In that context, more transparency and openness across the online advertising supply chain is a necessary first step to meaningfully address the variety of problems. It is worth noting that advertisers and publishers have been calling for many years for greater transparency across the supply chain (covering pricing and trading, fees and costs, placement and data usage), in order to better track advertising spend and to minimise brand risk (See for instance, the World Federation of Advertisers' Global Media Charter). This transparency mechanism could take the form of a public registry of advertisements and placements; publicly available ad archive APIs (which we explain in other parts of our submission); or dedicated transparency interventions with respect to the Real Time Bidding (RTB) mechanism.

Greater transparency would not only benefit advertisers and publishers. It would also enable regulators to better understand the dynamics and trends in the online advertising market and to gather insights that could: optimise tax treatment; identify and manage harmful commercial dependencies in multi-sided markets; better investigate complaints, and so forth. In addition, more transparency would be a boon for public interest researchers aiming at identifying and understanding how the online advertising ecosystem can engender harmful individual and social outcomes (e.g. harmful data collection practices; discrimination; etc).

One additional idea, proposed by the U.S.-based Stop Hate for Profit campaign (of which Mozilla is a supporting organisation), is to provide refunds to parties whose advertisements are presented to users next to policy infringing or illegal content that is subsequently taken down by the platform. While such an approach would better incentivise platform diligence of ad placement, it's hard to measure the degree of refunds or exposure involved with AI-based advertising systems that are not readily explainable. A public registry of ads and placement data could improve measurement of the underlying harm of unwanted ad placements, which may then clearly justify the provision of remedies, either voluntarily by platforms or through regulation.

15 From your perspective, what measures would lead to meaningful transparency in the ad placement process?

3000 character(s) maximum

We appreciate the focus on building additional transparency around ad placement in the EU. One methodology for increasing platform transparency in ad placement would be a framework whereby platforms that operate advertising networks publicly disclose all advertisements on their platforms via ad archive APIs.

If this approach was pursued, it could:
- Apply to all advertising, so as not to be constrained by arbitrary boundary definitions of 'political' or 'issue-based' advertising;
- Potentially include disclosure obligations that concern advertisers' targeting parameters for protected classes as well as aggregate audience demographics, where this makes sense given privacy and other considerations;
- Establish disclosure via publicly-available APIs, such that access is not restricted to specific privileged

stakeholders as we have seen in some existing ads transparency efforts.

Previous regulatory and co-regulatory initiatives aiming at ad transparency to combat disinformation have generally focused on ‘political’ advertising. Focusing on purely ‘political’ advertising (e.g. advertising copy developed by political parties) is too narrow an approach in many instances, and is often considered to be insufficient to capture the complex web of actors involved in politically-motivated disinformation online.

A broad ads disclosure framework could also drive transparency with respect to what is known as ‘issue’ advertising. Experience has shown how disclosure obligations that include this broader category of political ads put platforms in a challenging position, as the relevance for disclosure purposes of particular issue-based advertising requires platforms to decide what is 'political' in nature, which can vary depending on context, jurisdiction, and time. These problems can be avoided by disclosure of all advertisements. It avoids the risk of under-disclosure (that arises with overly narrow definitions); minimises the burden on platforms to make highly-contextual definitional assessments (that arises with definitions of ‘issue-based’ advertising); and, helps ensure that transparency objectives are resilient in the face of technological and commercial changes.

A thoughtful analysis of how to balance privacy considerations, business considerations, and transparency is necessary for a successful transparency landscape. The inclusion of targeting parameters and aggregate audience demographics can be a significant tool for ensuring that regulators and researchers can understand how disinformation can spread across platforms. For instance, for much of the disinformation that is delivered via advertising on platforms, the content of the advertising provides only a partial - and indeed ancillary - insight into the phenomenon. Rather, it is the fact of what types of individuals those advertisements are aimed at and under what circumstances, that can provide insight into the risks and harms.

16 What information about online ads should be made publicly available?

3000 character(s) maximum

Please see our answer to question 15, which suggests consideration of an approach where all online ads are disclosed in publicly available repositories, with a reasonable set of targeting parameters.

One important consideration in implementation will be how to best establish a framework that puts the onus on advertising platforms to publish ads in a reasonable way - without unfairly burdening small publishers or individual advertisers. We believe a careful discussion with stakeholders can drive reasonable thresholds for establishing greater transparency.

17 Based on your expertise, which effective and proportionate auditing systems could bring meaningful accountability in the ad placement system?

3000 character(s) maximum

Auditing systems are one possible means to bring accountability to the ad placement system. However, as we highlight in our response to question 14, we first need to have meaningful transparency into the online advertising value chain. Today the value chain is extremely opaque, and a baseline standard of transparency into how the system works holistically is a prerequisite for any framework that aims at auditing specific elements of that chain.

As a matter of principle, the regulatory framework should aim at public-facing disclosure of information related to advertising and ad placement where possible, with audits serving as, at best, a supporting or

complementary function. Researchers and watchdog groups should not have to ask permission to hold actors in the advertising ecosystem accountable, nor wait for whatever information is disclosed as the result of an auditing system. We believe the ecosystem and consumers are best served where stakeholders can have access to data that does not represent a security or privacy risk.

Governments have a critical role to play that can be effectuated with data about the advertising ecosystem. But governments alone may lack the expertise or resources to take full advantage. Instead, to hold actors in the advertising ecosystem accountable, those government bodies can take advantage of independent accountability organisations that have unmediated access to advertising data, and are best positioned to undertake robust analysis of the hidden harms and negative outcomes arising through the advertising ecosystem.

Finally, we also note that, while ad transparency is a foundational step to building platform accountability in advertising, more will need to be done to build governmental and NGO capacity. The capacity to actually take advantage of greater levels of transparency to better understand activity on ad platforms is currently lacking.

18 What is, from your perspective, a functional definition of ‘political advertising’? Are you aware of any specific obligations attached to 'political advertising' at national level ?

3000 character(s) maximum

‘Political advertising’ should be defined as a narrow set of advertisements that concern a specific public office holder, an electoral candidate, or a political party. As such, the definition hinges on the specific entity that is the subject or object of the advertisement.

There are a range of obligations attached to political advertising of this kind across the different EU Member States. While harmonisation is always preferred, we recognise the importance of granting individual member states the leeway to implement the electoral controls and safeguards that suit their specific electoral, political, and social context.

Yet, it is crucial to appreciate that the definition of political advertising above does not capture all advertising that is political in nature. This limitation is particularly important in cases where our objective is to limit the spread of dis- and mis-information around elections or to minimise electoral interference. In that respect, there are three principle short-comings of the narrow definition of political advertising that EU policymakers should be conscious of:

- This definition cannot account for the phenomenon of “issue based ads”. These are politically-charged advertisements on topics relevant to the election, that may not be paid for or be directly identified with a particular candidate or a particular political party. These advertisements are often key vectors for election-related disinformation.

- Narrow definitions of political advertising demand value judgements by platforms and continuous labelling of advertisements as ‘political’ or ‘non-political’. In virtue of the closed nature of online platforms; the broad definitions of ‘political’; and the variety of targeted advertisements means there is significant risk of ‘political’ advertising slipping through the transparency mechanism, with little ability for third parties to monitor for these slippages.

- There is a significant risk that both legitimate political actors and those seeking to spread misinformation

will game narrow definitions of political advertising to avoid disclosure obligations. Obligations around political advertising that rest upon narrow definitions are likely to quickly become outdated. The rise of social media 'influencer' political advertising is a case-in-point of the dynamic delivery mechanisms for political advertising today. Indeed, one consistent lesson we have learned from today's cybersecurity challenges is that attackers will seek to take advantage of holes in complex systems to adapt their behavior. A simpler, broader disclosure regime will limit attackers ability to adapt.

Of course, once this baseline is established, there would be merit in the EU exploring additional rules around political advertising and safeguarding electoral integrity (e.g. minimum security standards; verification obligations on social media for candidates; etc).

19 What information disclosure would meaningfully inform consumers in relation to political advertising? Are there other transparency standards and actions needed, in your opinion, for an accountable use of political advertising and political messaging?

3000 character(s) maximum

Please see our response to questions 15 and 18 of this section.

20 What impact would have, in your view, enhanced transparency and accountability in the online advertising value chain, on the gatekeeper power of major online platforms and other potential consequences such as media pluralism?

3000 character(s) maximum

A consistent theme in our responses has been that the advertising ecosystem is presently opaque, and that transparency can be an important first step to help us better understand and define policy responses to the negative outcomes.

It is unclear whether and to what extent greater transparency into the online advertising ecosystem will affect the power dynamics between the various market actors involved. That said, it is likely that the negative outcomes and bad practices that affect the ecosystem today may be contributing to market distortions, to the detriment of advertisers and publishers in particular.

For instance:

- Ad fraud: One of the biggest problems is the extent of fraud online today. Although the extent of fraud in today's advertising ecosystem is impossible to compute precisely, various estimates have put the figure at as high as USD 18 billion per year globally, with projections that it could rise to over USD 30 billion per year globally by 2023. Ad fraud is the product of various deceptive practices. For instance purveyors of ad fraud often deploy bot networks that artificially inflate click-throughs on programmatic advertising, with some estimates suggesting that over 40% of internet 'users' are bots deployed to advance ad fraud. This fraud is a major drag on the European economy, and likely the cause of considerable distortion in the online advertising ecosystem.

- Data leakage: Unfortunately harmful data gathering practices remain rife in the internet ecosystem, as participants in the advertising ecosystem seek to ever-more precisely target advertisements at internet users. Cross-site tracking and device fingerprinting are two of the well-known and problematic examples of this broader phenomenon of data leakage. For our part, we have been blocking third-party trackers through

the Firefox browser by default since September 2019, through our Enhanced Tracking Protection (ETP) technology.

Unfortunately the effort to combat cross-site tracking and other forms of data leakage in the online advertising ecosystem is akin to an arms race. With each technological solution Firefox deploys to address the problem, unscrupulous actors in the ecosystem develop increasingly problematic counter-measures to continue collecting excessive data. This is a problem which undermines the online advertising ecosystem as a whole - harming users and distorting market dynamics. Hopefully, an increased focus on transparency across the advertising value chain as well as a more robust enforcement of the GDPR can shed a light on the extent of data leakage, and inform effective technological and policy solutions to address it.

21 Are there other emerging issues in the space of online advertising you would like to flag?

3000 character(s) maximum

In closing, we would like to highlight that advertising is the dominant business model of the internet today, and it has fueled the development of a range of quality products and services that many of us rely on. Similarly, targeting and personalisation are key features of today's online experience, and when done properly they can allow us to navigate and discover the content and offerings that we want.

Yet the ecosystem underpinning these models and practices is unwell. Today the online advertising ecosystem is too often associated with pervasive cross-site tracking, ad fraud, and data leakage. Moreover, from political manipulation to bias and discrimination, we've seen too many instances of advertising microtargeting leading to real individual and collective harms and loss of trust. And because this advertising is so highly targeted, that harm is essentially hidden from public view.

The DSA is largely a product of this context, and we hope it will be a key mechanism by which the flaws in the current ecosystem can be addressed without undermining the good.

As a mission-driven tech company Mozilla is deeply invested in this debate. Like many other companies we benefit from advertising revenue, and we recognise that advertising-based business models are a necessary component of the open and sustainable web we care about. Yet we're equally committed to realising a web defined by privacy, security, and individual autonomy, and so cannot shirk from the policy effort to improve the advertising ecosystem.

As our responses to this section illustrate, we believe the first step in addressing the complex problems in the advertising ecosystem is transparency. We need greater transparency into the online advertising value chain, the logic of ad placement, and operation of the RTB mechanism. In addition, we need a clear framework for the bulk disclosure of advertising through publicly available ad archive API, to facilitate research and accountability efforts.

In the longer-run, EU policy should incentivise a structural shift towards contextual advertising, that has been shown to pose less public interest risk while maintaining returns for advertisers and ad hosts. The DSA, in conjunction with the GDPR and other regulatory and market-based initiatives, can set the course for that structural shift. An increasing body of evidence suggests that contextual advertising may not have a meaningful negative impact on publishers' revenue compared to behavioural advertising, and may indeed lead to increased financial returns. In addition, browser-level Enhanced Tracking Protection and Intelligent Tracking Protection effectively already shift the ecosystem towards contextual advertising without negative ramifications.

Increased transparency would serve as a crucial springboard for greater trust online, and would be particularly beneficial for publishers, advertisers, and ultimately consumers.

Smart contracts

1 Is there sufficient legal clarity in the EU for the provision and use of “smart contracts” – e.g. with regard to validity, applicable law and jurisdiction?

Please rate from 1 (lack of clarity) to 5 (sufficient clarity)	☆ ☆ ☆ ☆ ☆

2 Please explain the difficulties you perceive.

3000 character(s) maximum

3 In which of the following areas do you find necessary further regulatory clarity?

- ☐ Mutual recognition of the validity of smart contracts in the EU as concluded in accordance with the national law
- ☐ Minimum standards for the validity of “smart contracts” in the EU
- ☐ Measures to ensure that legal obligations and rights flowing from a smart contract and the functioning of the smart contract are clear and unambiguous, in particular for consumers
- ☐ Allowing interruption of smart contracts
- ☐ Clarity on liability for damage caused in the operation of a smart contract
- ☐ Further clarity for payment and currency-related smart contracts.

4 Please explain.

3000 character(s) maximum

5 Are there other points you would like to raise?

3000 character(s) maximum

V. How to address challenges around the situation of self-employed individuals offering services through online platforms?

Individuals providing services through platforms may have different legal status (workers or self-employed). This section aims at gathering first information and views on the situation of self-employed individuals offering services through platforms (such as ride-hailing, food delivery, domestic work, design work, micro-

tasks etc.). Furthermore, it seeks to gather first views on whether any detected problems are specific to the platform economy and what would be the perceived obstacles to the improvement of the situation of individuals providing services through platforms. This consultation is not intended to address the criteria by which persons providing services on such platforms are deemed to have one or the other legal status. The issues explored here do not refer to the selling of goods (e.g. online marketplaces) or the sharing of assets (e.g. sub-renting houses) through platforms.

The following questions are targeting self-employed individuals offering services through online platforms.

Relationship with the platform and the final customer

1 What type of service do you offer through platforms?

- ☐ Food-delivery
- ☐ Ride-hailing
- ☐ Online translations, design, software development or micro-tasks
- ☐ On-demand cleaning, plumbing or DIY services
- ☐ Other, please specify

2 Please explain.

3 Which requirements were you asked to fulfill in order to be accepted by the platform(s) you offer services through, if any?

4 Do you have a contractual relationship with the final customer?

- ○ Yes
- ○ No

5 Do you receive any guidelines or directions by the platform on how to offer your services?

- ○ Yes
- ○ No

7 Under what conditions can you stop using the platform to provide your services, or can the platform ask you to stop doing so?

8 What is your role in setting the price paid by the customer and how is your remuneration established for the services you provide through the platform(s)?

9 What are the risks and responsibilities you bear in case of non-performance of the service or unsatisfactory performance of the service?

Situation of self-employed individuals providing services through platforms

10 What are the main advantages for you when providing services through platforms?

3000 character(s) maximum

11 What are the main issues or challenges you are facing when providing services through platforms? Is the platform taking any measures to improve these?

3000 character(s) maximum

12 Do you ever have problems getting paid for your service? Does/do the platform have any measures to support you in such situations?

3000 character(s) maximum

13 Do you consider yourself in a vulnerable or dependent situation in your work (economically or otherwise), and if yes, why?

14 Can you collectively negotiate vis-à-vis the platform(s) your remuneration or other contractual conditions?

- Yes
- No

15 Please explain.

The following questions are targeting online platforms.

Role of platforms

17 What is the role of your platform in the provision of the service and the conclusion of the contract with the customer?

18 What are the risks and responsibilities borne by your platform for the non-performance of the service or unsatisfactory provision of the service?

19 What happens when the service is not paid for by the customer/client?

20 Does your platform own any of the assets used by the individual offering the services?

- Yes
- No

22 Out of the total number of service providers offering services through your platform, what is the percentage of self-employed individuals?

- Over 75%
- Between 50% and 75%
- Between 25% and 50%
- Less than 25%

Rights and obligations

23 What is the contractual relationship between the platform and individuals offering services through it?

3000 character(s) maximum

24 Who sets the price paid by the customer for the service offered?

- The platform

- [ ] The individual offering services through the platform
- [ ] Others, please specify

25 Please explain.

3000 character(s) maximum

26 How is the price paid by the customer shared between the platform and the individual offering the services through the platform?

3000 character(s) maximum

27 On average, how many hours per week do individuals spend offering services through your platform?

3000 character(s) maximum

28 Do you have measures in place to enable individuals providing services through your platform to contact each other and organise themselves collectively?

- ( ) Yes
- ( ) No

29 Please describe the means through which the individuals who provide services on your platform contact each other.

3000 character(s) maximum

30 What measures do you have in place for ensuring that individuals offering services through your platform work legally - e.g. comply with applicable rules on minimum working age, hold a work permit, where applicable - if any?
(If you replied to this question in your answers in the first module of the consultation, there is no need to repeat your answer here.)

3000 character(s) maximum

The following questions are open to all respondents

Situation of self-employed individuals providing services through platforms

32 Are there areas in the situation of individuals providing services through platforms which would need further improvements? Please rate the following issues from 1 (no improvements needed) to 5 (substantial issues need to be addressed).

	1 (no improvements needed)	2	3	4	5 (substantial improvements needed)	I don't know / No answer
Earnings	○	○	○	○	○	○
Flexibility of choosing when and /or where to provide services	○	○	○	○	○	○
Transparency on remuneration	○	○	○	○	○	○
Measures to tackle non-payment of remuneration	○	○	○	○	○	○
Transparency in online ratings	○	○	○	○	○	○
Ensuring that individuals providing services through platforms can contact each other and organise themselves for collective purposes	○	○	○	○	○	○
Tackling the issue of work carried out by individuals lacking legal permits	○	○	○	○	○	○
Prevention of discrimination of individuals providing services through platforms, for instance based on gender, racial or ethnic origin	○	○	○	○	○	○
Allocation of liability in case of damage	○	○	○	○	○	○
Other, please specify	○	○	○	○	○	○

33 Please explain the issues that you encounter or perceive.

3000 character(s) maximum

34 Do you think individuals providing services in the 'offline/traditional' economy face similar issues as individuals offering services through platforms?

- ○ Yes
- ○ No

I don't know

35 Please explain and provide examples.

3000 character(s) maximum

36 In your view, what are the obstacles for improving the situation of individuals providing services

1. through platforms?
2. in the offline/traditional economy?

3000 character(s) maximum

37 To what extent could the possibility to negotiate collectively help improve the situation of individuals offering services:

through online platforms?	☆ ☆ ☆ ☆ ☆
in the offline/traditional economy?	☆ ☆ ☆ ☆ ☆

38 Which are the areas you would consider most important for you to enable such collective negotiations?

3000 character(s) maximum

39 In this regard, do you see any obstacles to such negotiations?

3000 character(s) maximum

40 Are there other points you would like to raise?

3000 character(s) maximum

VI. What governance for reinforcing the Single Market for digital services?

The EU's Single Market offers a rich potential for digital services to scale up, including for innovative European companies. Today there is a certain degree of legal fragmentation in the Single Market . One of

the main objectives for the Digital Services Act will be to improve opportunities for innovation and '*deepen the Single Market for Digital Services*'.
This section of the consultation seeks to collect evidence and views on the current state of the single market and steps for further improvements for a competitive and vibrant Single market for digital services. This module also inquires about the relative impact of the COVID-19 crisis on digital services in the Union. It then focuses on the appropriate governance and oversight over digital services across the EU and means to enhance the cooperation across authorities for an effective supervision of services and for the equal protection of all citizens across the single market. It also inquires about specific cooperation arrangements such as in the case of consumer protection authorities across the Single Market, or the regulatory oversight and cooperation mechanisms among media regulators. This section is not intended to focus on the enforcement of EU data protection rules (GDPR).

Main issues

1 How important are - in your daily life or for your professional transactions - digital services such as accessing websites, social networks, downloading apps, reading news online, shopping online, selling products online?

Overall	☆ ☆ ☆ ☆ ☆
Those offered from outside of your Member State of establishment	☆ ☆ ☆ ☆ ☆

The following questions are targeted at digital service providers

3 Approximately, what share of your EU turnover is generated by the provision of your service outside of your main country of establishment in the EU?

- ○ Less than 10%
- ○ Between 10% and 50%
- ○ Over 50%
- ◉ I cannot compute this information

4 To what extent are the following obligations a burden for your company in providing its digital services, when expanding to one or more EU Member State(s)? Please rate the following obligations from 1 (not at all burdensome) to 5 (very burdensome).

	1 (not at all burdensome)	2	3 (neutral)	4	5 (very burdensome)	I don't know / No answer
Different processes and obligations imposed by Member States for notifying, detecting and removing illegal content/goods/services	○	○	◉	○	○	○
Requirements to have a legal representative or an establishment in more than one Member State	○	○	○	○	◉	○
Different procedures and points of contact for obligations to cooperate with authorities	○	○	○	◉	○	○
Other types of legal requirements. Please specify below	○	○	○	○	○	○

6 Have your services been subject to enforcement measures by an EU Member State other than your country of establishment?

- ○ Yes
- ◉ No
- ○ I don't know

8 Were you requested to comply with any ‘prior authorisation’ or equivalent requirement for providing your digital service in an EU Member State?

- ○ Yes
- ◉ No
- ○ I don't know

10 Are there other issues you would consider necessary to facilitate the provision of cross-border digital services in the European Union?

3000 character(s) maximum

While much consumer protection law in the various EU Member States is derived from Union-level regulations and directives, we note that the implementation and transposition of EU consumer protection laws can vary significantly across Member States. This fragmentation makes it difficult to offer services across the EU, particularly for start-up and scale-up companies.

11 What has been the impact of COVID-19 outbreak and crisis management measures on your business’ turnover

- ○ Significant reduction of turnover
- ○ Limited reduction of turnover
- ○ No significant change
- ○ Modest increase in turnover
- ○ Significant increase of turnover
- ○ Other

13 Do you consider that deepening of the Single Market for digital services could help the economic recovery of your business?

- ○ Yes
- ○ No
- ○ I don't know

14 Please explain

3000 character(s) maximum

The following questions are targeted at all respondents.

Governance of digital services and aspects of enforcement

The 'country of origin' principle is the cornerstone of the Single Market for digital services. It ensures that digital innovators, including start-ups and SMEs, have a single set of rules to follow (that of their home country), rather than 27 different rules.

This is an important precondition for services to be able to scale up quickly and offer their services across borders. In the aftermath of the COVID-19 outbreak and effective recovery strategy, more than ever, a strong Single Market is needed to boost the European economy and to restart economic activity in the EU.

At the same time, enforcement of rules is key; the protection of all EU citizens regardless of their place of residence, will be in the centre of the Digital Services Act.

The current system of cooperation between Member States foresees that the Member State where a provider of a digital service is established has the duty to supervise the services provided and to ensure that all EU citizens are protected. A cooperation mechanism for cross-border cases is established in the E-Commerce Directive.

1 Based on your experience, how would you assess the cooperation in the Single Market between authorities entrusted to supervise digital services?

5000 character(s) maximum

We have no specific insights to note.

2 What governance arrangements would lead to an effective system for supervising and enforcing rules on online platforms in the EU in particular as regards the intermediation of third party goods, services and content (See also Chapter 1 of the consultation)?
Please rate each of the following aspects, on a scale of 1 (not at all important) to 5 (very important).

	1 (not at all important)	2	3 (neutral)	4	5 (very important)	I don't know / No answer
Clearly assigned competent national authorities or bodies as established by Member States for supervising the systems put in place by online platforms	○	○	○	○	◉	○
Cooperation mechanism within Member States across different						

competent authorities responsible for the systematic supervision of online platforms and sectorial issues (e.g. consumer protection, market surveillance, data protection, media regulators, anti-discrimination agencies, equality bodies, law enforcement authorities etc.)	○	○	○	○	◉	○
Cooperation mechanism with swift procedures and assistance across national competent authorities across Member States	○	○	○	○	◉	○
Coordination and technical assistance at EU level	○	○	○	○	◉	○
An EU-level authority	○	◉	○	○	○	○
Cooperation schemes with third parties such as civil society organisations and academics for specific inquiries and oversight	○	○	○	○	◉	○
Other: please specify in the text box below	○	○	○	○	○	○

3 Please explain

5000 character(s) maximum

As we noted in our responses in section I.II, we believe that the DSA framework should be built around two key principles: procedural accountability; and a sliding scale of responsibility. While the DSA legislation can set the parameters and baseline meaning of these two principles, it will likely be the case that regulatory authorities (be they existing or new ones) will be required to operationalise and oversee their implementation.

While it should be the purview of companies to take the trust & safety measures that they feel are necessary for their specific risk-profile and business model, regulatory authorities have an important role to play in providing guidance, best-practice, and ultimately oversight of companies' efforts. Moreover, regulatory authorities have a role to play in ensuring that meaningful transparency and accountability are maintained in the DSA's implementation. For instance, our policy recommendations in section I.II call for greater transparency around advertising and content curation through recommender systems. We see a role for regulatory authorities to ensure that transparency is upheld, and where appropriate, undertaking the scrutiny of internal processes and systems that may be required. Furthermore, our firm belief is that regulators should focus their oversight on companies' practices – the steps they are taking to address illegal and harmful content on their service. Regulators should not have a role in assessing the legality or harm of individual pieces of content, and should not be empowered to issue takedown notices to companies. Such a role calls into play a number of critical legal and constitutional considerations, and exposes a real and significant risk of rights abuses. As such, when assessing companies' efforts under the DSA, the regulator should focus exclusively on practices and efforts, not content.

Given the political realities, it is likely most feasible that oversight and enforcement of rules be left to national-level authorities, working within an EU-wide framework of standards and coordination. We do not

have a particular preference as to whether the national-level oversight task should be undertaken by existing regulatory authorities or new special-purpose ones. Our primary desire is that regulatory authorities are given sufficient resources to reflect the breadth and complexity of their work, and that they are adequately staffed with suitable expertise from engineering, legal, data science, and social science backgrounds, amongst others. Further, the regulatory structure that oversees the DSA must ensure there is adequate appreciation and inclusion of the various policy equities involved in content governance. This issue space necessarily implicates audiovisual policy, consumer protection, data protection, competition, and so forth. The regulator tasked with overseeing the DSA at national level must be optimised to ensure these equities can be respected and harnessed.

With regard to the governance model for regulatory authorities in the DSA, multi-stakeholderism is essential. Companies themselves are likely to be best placed to understand the technological and operational solutions that can bring about a meaningful reduction in the relevant illegal or harmful content on their services. The governance model of regulatory authorities should acknowledge this reality, and ensure there are formal structures in place to allow meaningful co-regulation and dialogue between companies and the regulator. Moreover, the governance structure should ensure that civil society representatives are meaningfully included in the DSA's practical implementation. Civil society organisations should not merely be 'consulted' when the regulator develops policy or undertakes oversight actions. Rather, they should be integral to the process. Further to this, regulatory authorities' mission statements and terms of reference should also include a clear obligation to preserve internet openness and protection of citizens' fundamental rights.

Finally, it is a truism that the regulation of online content interferes with various fundamental rights. Given the comprehensive nature of the DSA and the fact that it will infer new powers on regulatory authorities, the risk of unjustified and disproportionate interference with individuals' fundamental rights increases. As a safeguard then, it is paramount that due process is built into the regulatory oversight system by design. This is particularly important with respect to the regulator's enforcement powers. Prior to issuing a sanction for breach of DSA obligations, the regulator must be obliged to meaningfully demonstrate that a breach has occurred, and companies must have recourse to an appeals mechanism and judicial process if they wish to contest the judgement. Moreover, regulatory guidance must be clear and foreseeable, to avoid a situation where companies are unable to ascertain what is required of them to ensure compliance

4 What information should competent authorities make publicly available about their supervisory and enforcement activity?

3000 character(s) maximum

Irrespective of how it is structured at national-level, regulatory authorities must be subject to parliamentary scrutiny and oversight. Each national-level regulator must be obliged to report regularly on its work to its national parliament, and the national parliament must be equipped with the power to summon the regulator and request specific information regarding its operations. In addition, regulators should be obliged to publish comprehensive reports on a regular basis that provide information on their investigatory and enforcement actions during the relevant period of time.

To ensure legal certainty and respect for the rule of law, the regulator should also publish comprehensive guidance on its oversight and enforcement strategy - i.e. what its regulatory objectives are; how it intends to allocate its oversight resources; and, the mechanisms by which it undertakes market surveillance and individual firm scrutiny. While these resources are likely only relevant for a particular audience (e.g. regulated companies and policy experts) they should nonetheless be made publicly available.

Finally, as we noted in our response to question 3 and in our responses in section I.II we believe that regulatory authorities have an important role to play in facilitating transparency in the platform ecosystem (e.

g. through acting as a clearing-house for access to platform data by researchers; undertaking targeted algorithmic systems inspections; etc). This could take numerous forms and will ultimately be determined by the type of transparency obligations the DSA legislation places on platforms.

5 What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms?

3000 character(s) maximum

As we note in our response to question 3, regulatory authorities must be given sufficient resources to reflect the breadth and complexity of their work. To that end, they should be staffed with suitable expertise from engineering, legal, data science, and social science backgrounds, amongst others. In addition, the regulatory structure and governance model must ensure there is adequate appreciation and inclusion of the various policy equities involved in the regulation of online content on contemporary services. Content regulation brings into play issues of audiovisual policy, consumer protection, data protection, competition, and so forth. The regulator tasked with overseeing the DSA at national level must be optimised to ensure these equities can be respected and harnessed.

6 In your view, is there a need to ensure similar supervision of digital services established outside of the EU that provide their services to EU users?

- ○ Yes, if they intermediate a certain volume of content, goods and services provided in the EU
- ○ Yes, if they have a significant number of users in the EU
- ◉ No
- ○ Other
- ○ I don’t know

7 Please explain

3000 character(s) maximum

Regulatory measures aimed at companies based outside of the EU jurisdiction should be conducted in line with principles of international law and the comity of nations, for instance, through mutual legal assistance treaties, and international trade agreements. The DSA should not bypass these norms.

8 How should the supervision of services established outside of the EU be set up in an efficient and coherent manner, in your view?

3000 character(s) maximum

See our response to question 7

9 In your view, what governance structure could ensure that multiple national authorities, in their respective areas of competence, supervise digital services coherently and consistently across borders?

3000 character(s) maximum

While we believe oversight and enforcement of the DSA should primarily take place at the national-level, an EU-level dimension is essential to ensure issues with cross-border impact can be appropriately managed and to avoid regulatory fragmentation.

In that context, we encourage the European Commission to explore whether the structures and approaches that we see in the fields of data protection and telecommunications regulation could be borrowed for the purpose of DSA oversight. While under the GDPR and the EU Electronic Communications Code national regulatory authorities retain primacy, those frameworks do facilitate a greater degree of cross-border cooperation, particularly with respect to information exchange and enforcement coordination.

Ensuring greater EU-level coordination of this kind will enhance effective enforcement and ensure the basic country-of-origin principle retains primacy in the single market.

10 As regards specific areas of competence, such as on consumer protection or product safety, please share your experience related to the cross-border cooperation of the competent authorities in the different Member States.

3000 character(s) maximum

11 In the specific field of audiovisual, the Audiovisual Media Services Directive established a regulatory oversight and cooperation mechanism in cross border cases between media regulators, coordinated at EU level within European Regulators' Group for Audiovisual Media Services (ERGA). In your view is this sufficient to ensure that users remain protected against illegal and harmful audiovisual content (for instance if services are offered to users from a different Member State)? Please explain your answer and provide practical examples if you consider the arrangements may not suffice.

3000 character(s) maximum

Given the type of products and services we offer, we do not engage with regulatory authorities regarding implementation of the EU Audiovisual Media Services directive.

12 Would the current system need to be strengthened? If yes, which additional tasks be useful to ensure a more effective enforcement of audiovisual content rules?
Please assess from 1 (least beneficial) – 5 (most beneficial). You can assign the same number to the same actions should you consider them as being equally important.

Coordinating the handling of cross-border cases, including jurisdiction matters	★★★☆☆

Agreeing on guidance for consistent implementation of rules under the AVMSD	
Ensuring consistency in cross-border application of the rules on the promotion of European works	
Facilitating coordination in the area of disinformation	
Other areas of cooperation	

13 Other areas of cooperation - (please, indicate which ones)

3000 character(s) maximum

14 Are there other points you would like to raise?

3000 character(s) maximum

Final remarks

If you wish to upload a position paper, article, report, or other evidence and data for the attention of the European Commission, please do so.

1 Upload file

The maximum file size is 1 MB
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

2 Other final comments

3000 character(s) maximum

Useful links

Digital Services Act package (https://ec.europa.eu/digital-single-market/en/digital-services-act-package)

Background Documents

(BG) Речник на термините

(CS) Glosř

(DA) Ordliste

(DE) Glossar

(EL) ά

(EN) Glossary

(ES) Glosario

(ET) Snastik

(FI) Sanasto

(FR) Glossaire

(HR) Pojmovnik

(HU) Glosszrium

(IT) Glossario

(LT) Žodynėlis

(LV) Glosārijs

(MT) Glossarju

(NL) Verklarende woordenlijst

(PL) Słowniczek

(PT) Glossrio

(RO) Glosar

(SK) Slovnk

(SL) Glosar

(SV) Ordlista

Contact

CNECT-consultation-DSA@ec.europa.eu