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.

This   **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 <u>a glossary</u>.

H o w   t o   r e s p o n d

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.

D e a d l i n e   f o r   r e s p o n s e s

8   S e p t e m b e r   2 0 2 0 .

L a n g u a g e s

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

Victoria

*4 Surname

DE POSSON

* 5 Email (this won't be published)

vdeposson@ccianet.org

* 7 Organisation name

255 character(s) maximum

Computer and Communications Industry Association (CCIA Europe)

* 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

11 Would you describe your company as :
- ☐ a startup?
- ☑ a scaleup?
- ☐ a conglomerate offering a wide range of services online?

12 Is your organisation:
- ☐ an online intermediary
- ☑ an association representing the interests of online intermediaries
- ☐ a digital service provider, other than an online intermediary
- ☐ an association representing the interests of such digital services
- ☐ a different type of business than the options above
- ☐ an association representing the interest of such businesses

☐ other

13 What type(s) of services do you provide?

☐ Internet access provider

☐ Domain name services

☐ Messaging service between a finite number of users

☐ Cloud computing services

☐ E-commerce market place: for sales of goods, travel and accommodation booking, etc.

☐ Collaborative economy platform

☐ Social networking

☐ Video, audio and image sharing

☐ File hosting and sharing

☐ News and media sharing

☐ App distribution

☐ Rating and reviews

☐ Price comparison

☐ Video streaming

☐ Online advertising intermediation

☐ Blog hosting

☑ Other services

14 Please specify

CCIA is an international, not-for-profit association representing a broad cross section of computer, communications and Internet industry firms. CCIA remains dedicated, as it has for over 45 years, to promoting innovation and preserving full, fair and open competition throughout our industry. Our members employ more than 1.6 million workers. For more, please go to: www.ccianet.org

15 What types of services does your platform intermediate?

☐ Temporary accommodation

☐ Private transportation

☐ Food delivery

☐ Household maintenance

☐ Other types of on-location services

☐ Software development

☐ Design

- ☐ Social media editing
- ☑ Other services provided online

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
- ☑ 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.

> 15987896534-82

*21 Country of origin

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

◉ Afghanistan	◉ Djibouti	◉ Libya	◉ Saint Martin
◉ Åland Islands	◉ Dominica	◉ Liechtenstein	◉ Saint Pierre and Miquelon
◉ Albania	◉ Dominican Republic	◉ Lithuania	◉ Saint Vincent and the Grenadines
◉ Algeria	◉ Ecuador	◉ Luxembourg	◉ Samoa

- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia

- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada

- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar/Burma
- Namibia

- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- 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

- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island

- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy

- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay

- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom

○ Clipperton	○ Jamaica	○ Peru	◉ United States
○ Cocos (Keeling) Islands	○ Japan	○ Philippines	○ United States Minor Outlying Islands
○ Colombia	○ Jersey	○ Pitcairn Islands	○ Uruguay
○ Comoros	○ Jordan	○ Poland	○ US Virgin Islands
○ Congo	○ Kazakhstan	○ Portugal	○ Uzbekistan
○ Cook Islands	○ Kenya	○ Puerto Rico	○ Vanuatu
○ Costa Rica	○ Kiribati	○ Qatar	○ Vatican City
○ Côte d'Ivoire	○ Kosovo	○ Réunion	○ Venezuela
○ Croatia	○ Kuwait	○ Romania	○ Vietnam
○ Cuba	○ Kyrgyzstan	○ Russia	○ Wallis and Futuna
○ Curaçao	○ Laos	○ Rwanda	○ Western Sahara
○ Cyprus	○ Latvia	○ Saint Barthélemy	○ Yemen
○ Czechia	○ Lebanon	○ Saint Helena Ascension and Tristan da Cunha	○ Zambia
○ Democratic Republic of the Congo	○ Lesotho	○ Saint Kitts and Nevis	○ Zimbabwe
○ Denmark	○ Liberia	○ Saint Lucia	

* 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

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

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)?

- ☑ 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')
- ☐ 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
- ☑ 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
- ☑ Other systems. Please specify in the text box below
- ☐ No system in place

2 Please explain.

5000 character(s) maximum

Internet services vary considerably and are ever-changing. For instance, some services pertain to video or images, some on selling products or on matching supply with demand, and others on enabling third-parties to offer services. Overall, each intermediary has specific systems/tools in place that are particularly effective for its particular services, and are proportionate to the level of potential risk of illegal content being offered or shared by users. The systems and tools used by intermediaries can differ between types of services, as they need to be tailored and efficient for the specific service concerned, and reflect the degree of knowledge and control that the intermediary has of the content on each service.

Automated tools have many advantages: In appropriate circumstances, they efficiently help companies identify content, products or conduct that conflict with their policies. It is however important to recognise the limitations of automated tools. For instance, they cannot be expected to understand the context of all types of content to the degree that a human reviewer may be able to. Equally, automated tools would struggle to examine the veracity of the claims made by a complainant. Human-intervention is therefore often essential to determine what can stay up, be brought down, or deactivated.

Independent 'third party' experts can play a key role in addressing the challenge of tackling illegal online content. When it comes to the concept of "trusted flaggers", it is essential to have a clear definition of their

roles, obligations and responsibilities. Furthermore, intermediaries must retain control of the appropriate reaction to a notification from a trusted flagger.

CCIA members are cooperating with a variety of national and regional authorities. As it can sometimes be unclear and challenging for small players to identify and verify the legitimacy of requests, we would welcome some harmonisation and clarifications helping tech companies to identify legitimate authority requests.

3 What issues have you encountered in operating these systems?

5000 character(s) maximum

The robustness of the content/product/conduct moderation practices lies in the complementary use of different tools. Each tool has strengths and weaknesses. When it comes to the challenges encountered in the operation systems, we can list:

- With notice-and-action systems, the challenges pertain to the fragmented legal approach amongst Member States. There is no clear definition as to what is considered a valid notice. It is extremely difficult for micro, small and medium-sized businesses to adapt to each local, regional and national rule. Another significant problem is non-valid notifications. When a content/product/conduct 'reviewer' receives a notification, the first objective is to identify the so-called problematic item and verify the veracity of the notification's claim.

- Verifying the veracity of claims also applies to content/products/conduct managed by automated tools. Indeed, filters can develop 'false positives' and leave some content/products/conduct up when it should be brought down, and vice-versa, bringing down lawful content/products/conduct.

- Fully automated tools can be particularly effective and time-efficient when (i) the content has been previously notified and removed, and; (ii) the circumstances leave no-doubt about the illegality of the material. Automated tools will be less efficient when contextualisation is required. For instance, an algorithm won't distinguish between war footage used by ISIS and the same footage used by human rights advocates. Furthermore, automatic stay-down procedures cannot, by definition, allow for context-related exceptions.

- A stronger and properly balanced EU harmonisation is needed on content/product/conduct moderation practices, to provide greater legal clarity and certainty, and to reduce the growing burden of complying with divergent Member State initiatives. A common EU framework would also support micro-businesses, SMEs, and digital service providers' growth and prosperity.

- Building a healthy and safe online environment is a societal challenge. Intermediaries, governments, right holders, civil society and users all have a role to play. Users and right holders should share their feedback and report problematic content, goods or conduct. Successful policy will ultimately depend on finding the appropriate balance between the rights and obligations of all relevant stakeholders. In parallel, intermediaries should continue to work with all sectors - industry, civil society and government - in order to have an impact on illegal content. This idea of a deeply collaborative approach should not be mistaken for an argument for 'self-regulation'. Rather, collaborative initiatives and legislative measures should co-exist to make the most of each of them.

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

Transparency reporting can be resource-intensive, particularly for smaller companies with fewer resources and employees.

Intermediaries have to verify the veracity of the notice. For instance, intermediaries routinely receive notices alleging content is illegal, which, after evaluation, prove to be incorrect. Vetting such incorrect notices requires resources that may be difficult, especially for smaller companies, to provide, and creates the risk of erroneous takedowns that harm users.

The fragmentation of the EU single market is an additional challenge. The methods used to evaluate content, goods or conduct can vary from one country to another, since it is not based on the same factors. For instance, the definition of illegal content differs from one country to another, so, as well as burdening SMEs with having to set up multiple transparency systems tailored to different Member States, it is difficult to generalise and compare the cost figure at EU level.

Numbers without context, especially on the prevalence of the problems in other channels of communication and commerce on- and off-line, can be misleading and could distract from addressing underlying challenges.

Overall, enforcement against the bad actors that misuse tools and attack the community of providers and users is under resourced. Prioritisation of these issues and resources for law enforcement is an important part of collective efforts.

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

The fragmentation of the EU single market makes it difficult to provide comparable transparency reports. As mentioned above, the definition of illegal content differs from one country to another, so it is challenging to generalise and compare such numbers at EU level.

Some CCIA members publish transparency reports highlighting the amount of different types of illegal content, services and goods notified, detected, removed, and reinstated, and the number of complaints received from users. For instance:
Amazon releases transparency reports on law enforcement information requests. It also posts updates on the proactive actions taken against counterfeits.
Facebook publishes quarterly Community Standards Enforcement reports.
Google shares transparency reports on content removal which include data on content delistings due to copyright, government requests to remove content or YouTube community guidelines enforcement.

Furthermore, the tech industry is very active in offering the best conditions to its sellers, users and consumers. Many CCIA members take part in voluntary measures such as the EU Internet Forum, the Global Internet Forum to Counter Terrorism (GIFCT), the Product Safety Pledge or the EU MoU on

Counterfeiting Online.

- The EU Internet Forum, which includes several CCIA members, including Facebook and Google, is one of the examples where the tech industry works hand in hand with EU officials and Member State authorities to build online trust and tackle online challenges such as terrorist content or child sexual exploitation.

- The Global Internet Forum to Counter Terrorism and its Hash Sharing Consortium is contributing to the fight against dissemination of terrorist content online. The Forum was among others founded by two CCIA members: Facebook and YouTube. It now counts 13 companies: Amazon, Ask.fm, Cloudinary, Dropbox, Facebook, Instagram, JustPaste.it, LinkedIn, Microsoft, Pinterest, Reddit, Snap, Twitter, Verizon Media, Yellow, and YouTube. The Forum partners with experts in government, civil society and academia. The Hash Sharing Consortium is a database which allows the sharing of "hashes" (or digital fingerprints) of known terrorist images and videos. In 2019, it reached over 200,000 unique pieces of terrorist content.

- Several CCIA members are signatories to the Code of conduct on countering illegal hate speech online. The aim of the Code is to make sure that requests to remove content are dealt with quickly. The companies commit to reviewing the majority of these requests in less than 24 hours and to removing the content if necessary, while respecting the fundamental principle of freedom of speech. The fifth monitoring report states that: "The IT companies fully meet the target of reviewing the majority of notifications within 24 hours. Facebook has reached 95.7% of notifications assessed within a day. On average, IT companies remove 71% of illegal hate speech incidents notified to them by the NGOs and public bodies participating in the evaluation."

- The Code of Practice on Disinformation has been signed by CCIA members Facebook and Google. The industry participants agree, on a voluntary basis, to self-regulatory standards to fight disinformation. It aims at achieving the objectives set out by the Commission's April 2018 Communication by setting a wide range of commitments, from transparency in political advertising to the closure of fake accounts and demonetisation of purveyors of disinformation. The 2019 annual assessment report indicates that significant efforts have been made by the signatories to implement their commitments.

- The tech industry is also very active in making sure that goods sold online are safe and not counterfeit. CCIA's marketplace members (Amazon, eBay, and Rakuten) have signed the European Commission's Product Safety Pledge which builds on the marketplaces' strengths such as increased traceability of products and the strong post-sale contact with customers, when needed. The second progress report stresses that on average, 93.56% of products identified by the marketplaces have been removed from their listings in two working days.

- Several CCIA members (e.g. Amazon, eBay, Facebook, and Rakuten) are signatories to the European Commission's Memorandum of Understanding on the sale of counterfeit goods via the internet. The MoU, in place since 2011, has contributed to reducing counterfeits online. The last report on the functioning of the MoU emphasises "that the MoU has effectively contributed to removing counterfeit products from online marketplaces and that it is a useful forum which allows trust and cooperation between parties to be strengthened".

- In the Intellectual Property Crime Threat assessment 2019, Europol and the EU Intellectual Property Office highlighted operational successes against anti-counterfeiting operations and emphasised the need for continued and enhanced private-public sector and law enforcement cooperation.

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

Different checks and balances are in place depending on the type of services and proportionate to the level of risk.

When examining the issue of reporting suspicious behaviours, it is vital to consider and protect the human rights and fundamental freedoms that would be impacted by such practices - including the data protection rights of the users concerned. Intermediaries will often not have sufficient context to determine whether behaviour genuinely amounts to steps in preparation for the commission of criminal acts. Neither do they have the expertise of law enforcement authorities, which are better placed to make such judgments. The consequences of reporting conduct which, without an adequate understanding of the context, might have appeared to be suspicious, but which in fact turned out to be entirely innocent, have the potential to be severe for the user concerned.

In the context of content moderation, fully automated tools can play a role in detecting and removing new identical copies of content that has been previously notified and removed, where the circumstances leave almost no-doubt about the illegality of the material. They can limit the spread of spam and other misleading and deceptive tactics designed to increase viewership.

On counterfeits and piracy, e-commerce services and online marketplaces have invested heavily in programs to address this challenge and enforce company policies against counterfeits and pirated goods. Existing measures taken by online e-commerce platforms include:

Brand registration programs: Some e-commerce-focused firms allow brand owners to voluntarily enroll in brand registration programs, which provide the service with automated tools to identify and remove confirmed counterfeit products. Through enrollment, the owners provide relevant information to the service about their products that better enables the service to proactively address counterfeits. Brands and digital services have also made joint referrals to law enforcement or launched co-litigation to address the counterfeiters that target both them and their customers.

Simplified notice and removal procedures: Online marketplaces have worked to make their reporting processes as efficient and easy as possible to facilitate swift removal of content that violates company policy. Verified right holders have a priority access to tools for expeditiously flagging and removing potentially infringing products.

Collaboration with brand owners: Online marketplaces work with brand owners and right holders through expanded programs that build upon tools like brand registration. For example, tools like "product serialization" have recently been introduced, to allow manufacturers to attribute a unique code to each product which is then verified by the online marketplace intermediary to confirm authenticity.

Other initiatives include transparency reports, trust and certification programs, or coordination with law enforcement.

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?
- ☑ 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

> Like other forms of technological innovations before it, the Internet can also be misused. We acknowledge the existence of rogue players who seek to inflict harm on others, whether seeking profit or promote hatred. Out of billions of interactions and conduct occurring through the use of digital intermediaries, only a tiny fraction are harmful. To handle those rogue players and remove problematic content, CCIA members continuously invest resources in technology and human review to keep their services safe and trustworthy from rogue players and illegal conduct. It is in our members' self-interest to expeditiously handle notifications to remove disinformation, fake news, or terrorist content from their platforms. CCIA members aim to allow each user to form its own judgements based on a variety of accurate and trustworthy content while all users have the opportunity to express themselves, conduct commerce or buy online.

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

3000 character(s) maximum

> Notice-and-action systems are essential to alert intermediaries of content that could be considered harmful. Based on the notifications, intermediaries can assess the need for intervention and potentially remove the content, based on their terms of service.
>
> Automated tools can be effective and time-efficient when the content has been previously notified, and the circumstances leave no-doubt about the harmful character of the material.

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

5000 character(s) maximum

> CCIA members are particularly attentive to content/products/conduct that could be considered as lawful but that could be used in an illegal manner. We believe that in order to strengthen trust online, intermediaries should be incentivised to act responsibly in tackling illegal content, products or conduct. Digital services should have the opportunity to take voluntary measures tackling problematic content, products or conduct without being penalised for their good faith efforts. It is critical not to limit this approach to content

moderation practices but unlock the opportunity to also do more to address social and safety concerns. Companies also place a lot of attention on the protection of minors online and have deployed specific channels that allow alerts related to this specific issue.

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

5000 character(s) maximum

Some CCIA members have tens of thousands of people working on content moderation, and have spent hundreds of millions of Euros on these efforts. Members are continuously developing their content policies and the measures necessary to combat policy violations, which each vary depending on (i) the nature of their services; (ii) the content in question, and; (iii) the associated risks for their users.

Intermediaries have to verify the accuracy of the information. For instance, intermediaries routinely receive notices alleging content is illegal, which after evaluation prove to be incorrect. Vetting such incorrect notices requires resources that may be difficult, especially for smaller companies, to provide, and creates the risk of erroneous takedowns that harm users.

The fragmentation of the EU single market is an additional challenge. The measurement of a similar element can vary from one country to another, since it is not based on the same factors. For instance, the definition of illegal content differs from one country to another, so, as well as burdening SMEs with having to set up multiple transparency systems tailored to different Member States, it is difficult to generalise and compare the figure at EU level.

Numbers without context, especially on the prevalence of the problems in other channels of communication and commerce on- and off-line, can be misleading and distract from addressing underlying challenges.

Overall, enforcement against the bad actors that misuse tools and attack the community of providers and users is under-resourced. Prioritisation of these issues and resources for law enforcement is an important part of collective efforts.

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

CCIA members aim to maintain respectful digital environments for everyone. Users of those environments must follow the relevant platform's basic rules of conduct. Many of which specifically call out bullying and harassment, and provide tools for reporting those who don't follow the rules. CCIA members also provide resources for users, parents and educators seeking support for issues related to bullying and other conflicts.

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

The measures taken when a user disputes the removal of their goods or content or service vary depending on (i) the type of the user, e.g. business user or consumer user; (ii) the type of content, product, and service, and; (iii) the channel used by the user to appeal the decision.

First of all, the appeal system for business users falls within the legal framework of the recent EU Regulation on fairness and transparency in online platform-to-business relationship ("P2B"). The new Digital Services Act should ideally be aligned with this existing regulation and not re-open this file which companies and authorities have just spent significant resources to implement.

Secondly, measures taken when a user disputes the removal of their goods or content or service vary according to the type of content, goods and conduct/services. It is important to assess the problematic content/product/conduct in view of the context, which can be determining for the decision to leave it up or take it down.

In addition, it is important to acknowledge and differentiate between various types of intermediation services. There are, according to European Commission estimates, approximately 10,000 platforms and marketplaces operating in the EU Single Market. This enormous diversity should be properly accounted for in the context of any changes to the existing legal framework. For instance, a cloud or a technical infrastructure provider does not provide the same services as a content hosting service, and the extent to which they can be said to have both legal and technical control over information may be very different.

Thirdly, some intermediaries have developed appeal systems/procedures and channels which are most effective to ensure trust on their specific type of services. A targeted and problem-solving approach in the DSA would therefore be more appropriate than a one-size-fits-all approach.

Furthermore, when it comes to the level of detail of the statement of reason (explanation given to business users that their content/product or account has been removed or deactivated), CCIA supports proportionate transparency requirements that strike a balance between the need for transparency, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets. The extent of information provided to the disputed party should be limited to what is strictly necessary without undermining third-parties' rights to the confidentiality and protection of their personal data, in line with the General Data Protection Regulation (GDPR).

We would welcome a clear definition of what should constitute a "counter-notice". When developing such a definition, policy-makers should create a framework that avoids adding unnecessary complexity to the process.

We would generally welcome proportionate and horizontal measures that focus on the processes and the

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

The quality standards and control mechanisms are specific to the type of intermediary, content, product, and services. Generally, automated systems have been trained on hundreds of thousands, if not millions, of different examples of violating content and common attacks.

Notice-and-action frameworks established an efficient means of removing any allegedly infringing content quickly from internet services, while fostering cooperation among relevant stakeholders.

CCIA members work continuously to ensure their users' trust in their services. For content, members have for instance developed various systems such as YouTube Content ID, the Google Search Trusted Copyright Removal Program and the Facebook Rights Manager. In the context of trademark protection, major e-commerce providers also voluntarily provide legal tools for IP protection by brand owners. These initiatives include the eBay Verified Rights Owner program, the Amazon Brand Registry and the Facebook Commerce and Ads IP Tool.

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

CCIA members have various measures in place. Generally speaking, when a notice takes place, the intermediary service will expeditiously assess the legality of the content/product/conduct and decide to leave it up or take it down. Based on its assessment, the intermediary service provider will inform the relevant players of its decisions. The players can then decide to appeal this decision, and go to a mediator if needed.

A few CCIA members are also part of the Global Network Initiative (GNI), which aims to protect and advance freedom of expression and privacy rights by setting a global standard for responsible decision making and serving as a multistakeholder voice in the face of government restrictions and demands. GNI brings together ICT companies, civil society (including human rights and press freedom groups), academics, academic institutions, and investors from around the world to provide a framework for responsible company decision making, foster accountability by member companies, offer a safe space for shared learning, and provide a forum for collective advocacy in support of laws and policies that promote and protect freedom of expression and privacy.

D. Transparency and cooperation

1 Do you actively provide the following information:

- ☑ Information to users when their good or content is removed, blocked or demoted
- ☑ 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?
- ☐ Notices received from third parties?
- ☐ Referrals from authorities for violations of your terms of service?
- ☐ Removal requests from authorities for illegal activities?
- ☐ 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

> The measures taken to handle problematic content, products, conducts or services are very specific to the type of content, goods and conduct/services. Furthermore, the specificities of the type of service provided by the intermediary also influence the approach and procedures chosen. The transparency reports reflect this variety of ways of functioning. Having horizontal measures and a "one-size-fits-all approach" in transparency reports could harm the operations and efficiencies of the measures. Any transparency obligations should be proportionate to the services offered and the associated level of risks, particularly in light of how resource-intensive these requirements can be.
>
> We believe that in order to enhance trust online, intermediaries should be incentivised to act responsibly in tackling illegal content, products or conduct. Digital services should have the opportunity to take voluntary measures tackling problematic content, products or conduct without being penalised for their good faith efforts. It is critical not to limit this approach to content moderation practices but unlock the opportunity to do more on the social and safety front.
>
> We would be open to discuss transparency requirements for content moderation and recommender systems. Many CCIA members already regularly publish transparency reports on their content moderation practices and outcomes. When calling for more transparency, it is important to aim for meaningful transparency with a

fair purpose. Policy-makers should be mindful to not overwhelm consumers, businesses or authorities.

CCIA supports proportionate transparency requirements that strike a balance between the need for transparency, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets.

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

The use of automated tools varies depending on the type of content, product, conduct, and on the specificities of the service provided by the intermediary. The transparency reports reflect this diversity. Having horizontal measures and a "one-size-fits-all approach" in transparency reports could harm the operations and efficiencies of the measures.

However, fully automated tools are only effective and time-efficient when the content has been previously notified, and the circumstances leave no-doubt about the illegality of the material. As soon as there seems to be a grey-zone, the content/product/conduct is handled by humans as they are able to contextualise the situation.

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

Disclaimer: CCIA limits its response to questions 6 and 7 to data sharing and reporting practices where data constitutes unlawful content. For any information on data access and sharing with third-parties for other reasons and where data does not constitute unlawful content (e.g. commercial, research, etc.) and portability requests, we refer to our previous contributions:
https://www.ccianet.org/wp-content/uploads/2020/06/FINAL-Supplementary-comments-CCIA-submission-on-EC-Data-Strategy-Consultation.pdf
https://www.ccianet.org/wp-content/uploads/2020/07/CCIA-Response-Finnish-Data-Economy-Principles-Paper.pdf

(1) Mandatory reporting of unlawful content/products to law enforcement authorities/competent authorities, for information society service ('ISS') providers:

CCIA members cooperate with national authorities when they receive legitimate data requests (e.g. criminal investigations) as per national laws. Should the request involve personal data, then ISS may only provide said data if the legislation meets the conditions in Article 23 of the General Data Protection Regulation (GDPR), and to the extent that it is consistent with relevant applicable third country laws (e.g. blocking statutes). Beyond the grounds set out in Article 23(1) GDPR, companies may only be authorised to provide personal data to competent authorities as per Article 6(1) GDPR.

(2) Mandatory reporting of unlawful content to law enforcement authorities/competent authorities, for Electronic Communication Service ('ECS') Providers:

Until December 2020, ECS providers may report data constituting unlawful content to national competent authorities as per the conditions set out above. As of December 2020, and pending the adoption of further EU legislation, ECS providers may only report and share data with national competent authorities if national laws exist, providing they meet the conditions in Article 15(1) of the e-Privacy Directive.

(3) Voluntary reporting of unlawful content/products to law enforcement authorities/competent authorities:

Companies may report unlawful content or products to competent authorities on a voluntary basis, to the extent possible under GDPR and/or the e-Privacy Directive. We encourage the European Commission to provide companies with greater comfort with how information sharing can be conducted whilst appropriately balancing the human rights and fundamental rights potentially impacted by such disclosures.

(4) Voluntary data sharing with third-parties for the purpose of detection of unlawful content and subsequent reporting:

Companies are increasingly developing and/or contributing to shared repositories of unlawful content to improve companies' detection and reporting rates. The governance framework and third-party participation may vary depending on each scheme. Participation in PhotoDNA to detect Child Sexual Abuse Material is subject to contractual agreements granting access to APIs. Contractual agreements are also in place for commercial solutions which pool real-time cybersecurity attacks for instance. On the other hand, the EU and Global Internet Forum's fight against terrorist and violent criminal content involve collaborations between companies, representatives of the civil society, and public authorities.

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, only platforms	

	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	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

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?

☑ Precise location: e.g. URL

☑ Precise reason why the activity is considered illegal

☑ Description of the activity

☑ 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

The more relevant information that intermediaries receive in a notification, the more effectively they will be able to take necessary measures. A notifier should be as specific as possible in identifying the content (including the URL), identifying the relevant law, identifying the notifier and their status, justifying why content should be brought down, and attesting to the good faith of the claim. Notifications without a minimum of information shouldn't be considered valid notice.

Additionally, in order to protect intellectual property and copyrights, right holders should provide evidence of their rights in the specific jurisdiction, in order to help intermediaries identify breaches and bring the content down.

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

Notice and takedown should remain the central approach to addressing illegal content. The prohibition against imposing general monitoring obligations should be preserved. Rather than incentivising intermediaries to block lawful content to protect themselves from potential sanction, which would adversely impact the fundamental rights of EU citizens, intermediaries should instead be incentivised to engage in reasonable and proactive voluntary actions to address illegal content, goods or services.

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?

Automated tools have many advantages: In appropriate circumstances, they efficiently help companies identify content, products or conduct that conflict with the provider's policies. However, it is important to recognise their limitations. For instance, they cannot be expected to understand the context of all types of content to the degree that a human reviewer may be able to. Equally, automated tools would struggle to examine the veracity of the claims made by the complainant in a meaningful way. Human-intervention is therefore often essential to determine what can stay up, be brought down or deactivated.

Independent 'third-party' experts can play a key role in addressing the challenge of tackling illegal online content. When it comes to the concept of "trusted flaggers", it is essential to have a clear definition of their roles, obligations and responsibilities. Furthermore, intermediaries must retain control of the appropriate reaction to a notification from a trusted flagger.

Overall, online intermediaries should not generally be asked to police and remove content unless a specific report for an individual piece of content is received. Otherwise, online intermediaries will, where they are available, need to rely on automated tools and technologies that may not be fit for purpose or fully developed, resulting in a vast number of false positives and over-blocking. For this reason, requests should be limited to circumstances where risks of severe harm exist due to the nature of the content and removal is the best and only option.

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?

CCIA supports the European Commission's objective to treat all digital services equally when services target EU consumers, regardless of where they are established.

We agree with the Commission's inception impact assessment, which seeks to "clarify and upgrade the liability and safety rules for digital services and remove disincentives for their voluntary actions". We argue that the current framework actually creates an unreasonable incentive for companies to either refrain from

taking reasonable proactive moderation, or to over-remove content in the course of moderating. Just because a company (in good faith) seeks to find and remove illegal content, this should not imply that the platform has full knowledge of all unlawful content on its platform.

We argue knowledge should continue to be based on notices. If a company does have knowledge of an alleged illegal piece of content based on notice, then the company must decide whether to remove such piece of content or not.

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

CCIA supports the proportionate and targeted approach suggested by the European Commission. We wouldn't be opposed, in principle, to the creation of specific graduated categories for different platform types, that reflect the nature of the service provided and the degree of knowledge and control that the service has over individual items of content, in order to prevent fragmentation between the Member States. However, we strongly oppose defining a category of responsibility based on the size of a given intermediary. This would incentivise successful European players to stay small to avoid regulation. Another unintended consequence would be fragmentation and the migration of illegal content, goods or conduct to smaller, less regulated platforms (including those not established in the EU). We strongly support the Commission's intention of removing "disincentives for their voluntary actions to address illegal content, goods or services they intermediate."

We would welcome horizontal measures focusing on the processes and the underlying principles. That has been the enduring success of the ECD. Specific measures concerning types of content, goods or collaborative economy services should be considered individually and across on- and off-line spaces in order to address root causes.

Furthermore, it is essential to acknowledge and differentiate between the various types of intermediary services. These should properly be accounted for in the context of any amendments made to the currently applicable framework. For instance, a cloud or technical infrastructure provider does not provide the same services as a content hosting service, and the extent to which they can be said to have control over information may be very different.

We would support a European problem-solving approach based on stakeholder consultation, evidence and thorough assessment. To be effective in assessing providers' responsibilities, a pragmatic and targeted approach would be preferable.

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

The evidence of the self-regulatory activities, documented through several MoUs and Codes of Practices, is that online intermediaries can and do seek to play a role when it comes to tackling all kinds of problematic content, products or conduct. While online companies must play their part, there are also responsibilities for

law enforcement, rights owners or users. Bringing illegal content down is a community effort:

First, national authorities should be well-equipped to identify and assess the legality of certain types of content (i.e. unsafe products).

Users and right holders should share their feedback and report problematic content, goods or conduct.

Successful measures will ultimately depend on finding the appropriate balance between the rights and obligations of all relevant stakeholders. We believe it is a community effort and therefore all actors on the value chain should be considered when regulating illegal 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

CCIA suggests treating 'illegal' and 'lawful but harmful' content/product/conduct differently. 'Lawful but harmful' content/product/conduct cannot be treated as 'illegal' content as it may lead to infringements of important rights, such as freedom of expression and access to information.

Harmful content is complicated to assess, as definitions are vague and norms often vary considerably, even amongst EU Member States.

We propose a targeted regulatory approach adapted to the type of content in question, since this will be more effective and limit the risk of unintended consequences. We believe that the Digital Services Act should focus on tackling illegal content, products and conduct online.

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

CCIA members are working hard everyday to strengthen trust online and guarantee consumers' safety and security. Their measures are proportionate to the known risks and are regularly evaluated to match the reality on the ground.

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

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?

In the context of COVID-19, several CCIA members have taken a vast array of measures including automated, and where necessary, human monitoring of the content displayed in relation to various keywords and a categorisation of products at risks of being scams. Price gouges are addressed by algorithms and general preventive measures are taken to ensure traders are properly informed of possible unfair practices. CCIA members made temporary bans on the selling or advertising of specific products such as masks or alcoholic gels, they listed only the confirmed and reputable providers of certain products. In addition, many of our members launched consumer and seller information campaigns and safety resources in line with official expertise and governmental advice about COVID-19. A significant number of products/offers/ads were withdrawn, up to one million in a week by the biggest operator, with hundreds of thousands of price gouges detected. CCIA members created dedicated teams to address the crisis and evolution of practices and to proactively, including on a 24/7 basis, monitor developments on their platforms with regular sweeps (including through work with European enforcement agencies).

For more detail see March 23, 2020 letters to Commissioner Didier Reynders from CCIA members Amazon, eBay, Facebook, Google, Rakuten and Verizon Media (Yahoo). For instance, as of 29 July 2020, eBay blocked or removed more than 31 million listings that violated its Coronavirus policies.

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

It is important for service providers to provide sufficient transparency into how their systems are performing to give the community visibility and to monitor the dynamics of content, so that we can continually improve. However, the type and nature of what should be made transparent should not be so fixed as to predetermine the nature of the platform. Transparency should avoid being overly detailed with regard to automated systems or how enforcement measures operate as doing so could allow bad actors to circumvent the systems. Different types of services may require different levels of transparency, and needs to be proportionate according to the characteristics and nature of the provider.

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

CCIA members have measures in place aiming at strengthening trust online and guaranteeing consumers' safety and security. These measures are proportionate to the known risks and are regularly evaluated to match the reality on the ground.

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

CCIA would be open to discuss transparency requirements for (automated) content moderation and recommender systems. Many CCIA members already regularly publish transparency reports on their content moderation practices and outcomes.

When calling for more transparency, it is important to aim for meaningful transparency pursuing a fair

purpose. CCIA supports proportionate transparency requirements that strike a balance between the need for transparency, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets. We moreover do not want to overwhelm consumers, businesses or authorities.

Furthermore, any transparency and reporting obligation must adhere to existing EU legislation and fundamental rights. The alleged asymmetries in information, as mentioned in the inception impact assessment, should be assessed taking into account EU data protection rules, the need for better enforcement of existing tools (GDPR).

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

As mentioned in the previous question, we would be open to discuss transparency requirements for (automated) content moderation and recommender systems. Many CCIA members already regularly publish transparency reports on their content moderation practices and outcomes.

When calling for more transparency, it is important to aim for meaningful transparency pursuing a fair purpose. CCIA supports proportionate transparency requirements that strike a balance between the need for transparency, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets. We moreover do not want to overwhelm consumers, businesses or authorities.

Furthermore, any transparency and reporting obligation must adhere to existing EU legislation and fundamental rights. The alleged asymmetries in information, as mentioned in the inception impact assessment, should be assessed taking into account EU data protection rules, including the need for better enforcement of existing tools (GDPR).

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

5000 character(s) maximum

We agree that it is important to give users a fair sense of how data is used and for what purposes. It is also important to be open about how content is organised and prioritised for them, including by algorithmic recommender systems. As users seek more transparency and control over their online experience, CCIA members are developing tools to address these needs.

The regulatory approach to algorithmic recommender systems needs to be balanced and not overly-prescriptive. As a tool, transparency has potential for both positive and negative impact. It can empower users but amongst those there will also be bad actors who will use information on algorithmic transparency to manipulate the algorithms. It is important that policy-makers be careful in demanding levels of transparency that risk making the algorithmic systems vulnerable to manipulation. Any such obligations should be proportionate to the services offered and the associated level of risks.

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

☐ 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

> We support proportionate transparency requirements that strike a balance between the need for transparency, the protection of users' fundamental rights, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets.
>
> We would be concerned about any proposals that seek to circumvent existing legal protections or require intermediaries to disclose user data without prior oversight by an independent authority and without proper legal safeguards.

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

> A positive user experience is key to the success of any commercial service offering. Accordingly, companies are already motivated to utilise effective systems to ensure compliance with their obligations. Where the threat of sanctions, in order to encourage compliance, is deemed strictly necessary, such sanctions should only apply where there is evidence of sustained failure to comply with clear obligations. The sanctions should be proportionate, and any sanctions regime should not incentivise the blocking of lawful content, nor have an adverse impact upon the fundamental rights of users.

24 Are there other points you would like to raise?

3000 character(s) maximum

We would also like to stress the EU 'better regulation' principles. We encourage policy-makers to consult stakeholders, conduct robust impact assessments, and then act based on clear evidence. Any new initiative should be based on proper consultations with stakeholders and a thorough consideration of empirical evidence if it does not want to inadvertently create harm. Legislators should carefully assess any potential unintended consequences that regulating digital services might have on businesses operating in Europe, particularly SMEs. Obligations should be achievable, and proportionate to known risks. This should also reflect the need for sufficient protections for users' rights of freedom to do business and freedom of speech, and to prevent over-blocking as the default response to obligations and any regulatory oversight.

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.

1 How important is the harmonised liability exemption for users' illegal activities or information for the development of your company?

Please rate from 1 star (not important) to 5 stars (very important)	⭐ ⭐ ⭐ ⭐ ⭐

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

We would welcome horizontal measures focusing on the processes and the underlying principles. That has been the enduring success of the e-Commerce Directive (ECD). Specific measures concerning types of content, goods or collaborative economy services should be considered individually and across on- and off-line spaces in order to address root causes.

It is essential to acknowledge and differentiate between the various types of intermediary services. These should properly be accounted for in the context of any amendments made to the currently applicable framework. For instance, a cloud or technical infrastructure provider does not provide the same services as a content hosting service, and the extent to which they can be said to have control over information may be very different.

CCIA supports the proportionate and targeted approach suggested by the European Commission. We wouldn't be opposed in principle to creating specific graduated categories for different platform types, that

reflect the nature of the service provided and the degree of knowledge and control that the service has over individual items of content, in order to decrease fragmentation between the Member States. However, we strongly oppose defining a category of responsibility based on the size of market power. The risk of such an approach could be to incentivise successful players to stay small in the EU to avoid regulation. Another unintended consequence would be fragmentation and the migration of illegal content, goods or conduct to smaller, less regulated platforms (including those not established in the EU). We strongly support the Commission's notion of removing "disincentives for their voluntary actions to address illegal content, goods or services they intermediate."

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 encourage an innovation-friendly framework to help digital service providers to develop, scale up in the EU single market and compete globally. A harmonised EU framework would support micro-businesses, SMEs, and digital service providers' ability to innovate and grow. In an assessment of the ECD, CCIA would welcome clarifications and harmonisation of 'notice-and-takedown' procedures, and ensure they complement the concepts of 'actual knowledge' and 'manifestly illegal content'.

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

We agree with the Commission's inception impact assessment, which seeks to "clarify and upgrade the liability and safety rules for digital services and remove disincentives for their voluntary actions". We believe the current framework creates an unreasonable incentive for companies to either refrain from taking reasonable proactive moderation, or to over-remove content in the course of moderating. Just because a company tries (in good faith) to find and remove illegal content, this should not imply that the platform has full knowledge of any unlawful content on its platform.

We believe knowledge should continue to be based on notices. If a company does have knowledge of an illegal piece of content based on notice, then the company should decide whether to remove such piece of content or not.

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

As highlighted in the Institute of Information Law report on Hosting Intermediary Services and Illegal Content Online [p. 31], the passive service provider concept in Recital 42 was a reference to Articles 12 (mere conduit service providers) and 13 (caching service providers). Extending the concept to Article 14 (hosts)

has led to a confusing and ultimately unhelpful distinction between "active" and "passive" hosts. This has created significant uncertainty and liability risk in relation to common features expected by today's users of intermediary services. Further, it has had the unfortunate result of leading some national courts to stray away from determining the core legal issue of whether the host in question had actual knowledge or awareness relating to the specific information or activity in issue.

CCIA would welcome the clarification of Recital 42. We would support doing away with the active/passive distinction in the DSA, and would support reaffirmation of the fact that the core test is one of actual knowledge.

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

The Digital Services Act will likely impact what can be read, sold or offered through digital intermediaries, and the types of real-life gatherings that online platforms help facilitate, hence we have to ensure the respect of fundamental rights and principles such as the freedom of expression. Policy-makers should weigh the legality, legitimacy, and necessity of the measures aimed at ensuring trust online. For instance, prioritising speed over proper deliberation and consultation often contributes to imprecise definitions, regulatory uncertainty, and distrust. A collaborative approach around legitimate policy objectives should prevent unintended consequences that can hinder innovation and the growth of digital services. Human rights experts have long identified proactive monitoring and filtering as serious potential threats to internet users' rights, including free expression, information access, freedom from discrimination, and privacy. It is important that the Digital Services Act respects these fundamental rights.

Intermediaries should not be held directly liable for what their users do. A general monitoring obligation could lead to excessive takedowns or deactivations. It would also likely lead to a market entry barrier as startups and SMEs would likely not have the technical means and the legal capacity to implement a general monitoring obligation which would harm innovation and competition. A 'no obligation to monitor' rule is the necessary companion of the liability protection principle. The Digital Services Act should under no circumstances weaken these fundamental principles which are widely used in democratic societies.

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

CCIA members are particularly attentive to content/products/conduct that could be considered as lawful but that could be used in an illegal matter. We believe that in order to strengthen trust online, intermediaries should be incentivised to act responsibly in tackling illegal content, products or conduct. Digital services should have the opportunity to take voluntary measures tackling problematic content, products or conduct without being penalised for their good faith efforts. It is critical not to limit this approach to content moderation practices but unlock the opportunity to also do more to address social and safety concerns.

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

Gatekeeper power suggests the ability to foreclose access to a market, that means that the platform is indispensable for suppliers to compete on the market in which they provide their products and/or services. In this respect, CCIA broadly agrees with the CMA's assessment that a "gatekeeper" designation should be limited to undertakings with "a position of enduring market power over a strategic bottleneck or gateway market, where a firm controls others' market access and where there are many dependent users on either side." CMA "Call for Information on the Digital Markets Taskforce" (1 July 2020), para. 2.5, citing Digital Competition Expert Panel "Unlocking digital competition" (March 2019) ("Furman Report"), paras. paragraphs 2.10, 2.25-2.27 and 3.69. See also Furman Report, para. 2.116 ("This needs to be carefully designed to identify where companies operating platforms are in a position to exercise potentially enduring market power, without granting an excessively broad scope and bringing within the bounds of regulation those companies who are effectively constrained by the competitive market.")

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

The existing competition case-law on "essential facilities" is instructive, particularly where the access remedies are envisaged. Essential facilities case-law has developed a careful framework for assessment that balances the rights of right holders, incentives to innovate and invest, and broader interests in the competition process. It serves as an existing, internationally recognised framework with concepts familiar to competition enforcers. In this regard, with respect to "gatekeepers", it requires not only evidencing market power, but also a demonstration of indispensability. According to the existing antitrust framework, indispensability means there is no actual or potential substitute on which competitors in the related market could rely, i.e. no economically feasible alternative means of distribution. This finding should be time-limited and can be revised, also at the request of the encumbered undertakings, as market circumstances develop. This ensures that undertakings remain incentivised to develop, and invest in, their own products and

services without fear that competitors will appropriate the value of these investments. Failure to meet these criteria would undermine the notion that "the right to choose one's trading partners and freely to dispose of one's property are generally recognised principles ... in some cases with constitutional status. Incursions on those rights require careful justification." When mandating access to private resources, such an approach would protect against these regulations being used to (a) subsidise or protect incumbent industries suffering from their own unwillingness to adapt to technological disruption, or (b) give competitors a free ride on the pro-competitive investments of private companies.

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:

- ☐ 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
- ☐ operating systems for smart devices
- ☐ consumer reviews on large online platforms
- ☐ network and/or data infrastructure/cloud services
- ☐ digital identity services
- ☐ 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

As mentioned above, CCIA submits that a "gatekeeper" designation implies control over an enduring strategic bottleneck necessary for others' access to a market. Accordingly, the key question is to identify the existence of such a strategic bottleneck. Additional products or services ancillary to that bottleneck are not relevant for the assessment of whether the bottleneck exists. If a bottleneck exists, adjacent markets /conglomerate effects may be where market power is exerted or monetised (e.g. through anticompetitive tying), but this is more to do with the assessment of conduct/application of prohibitions, rather than the "gatekeeper" designation. In any case, this would need to be subject to a case-by-case assessment and cannot be done in the abstract.

Emerging issues

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

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

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

No

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

3000 character(s) maximum

No

---

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

5000 character(s) maximum

> No

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

> The data economy continues to develop, innovation is rapid, and competition is dynamic. The General Data Protection Regulation (GDPR) and the Regulation on fairness and transparency in online platform-to-business relationship ("P2B") have increased transparency and accountability with regards to the use and sharing of data. We do not see any particular challenges given the state of technology as it is today and existing competitive incentives.

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

3000 character(s) maximum

> In general, we are not aware of unfair practices having a disproportionate impact on innovation, competition and consumer choice in the digital context, as compared to legacy distribution models. Markets appear to be working and there are high levels of innovation, competition and consumer choice in the single market. In any case, any potentially negative impact would need to be assessed on a case-by-case basis and cannot be generalised across industries.

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

> Digital intermediaries' services help startups and scale-ups grow their business and there would not be as many SMEs today if not for the innovations and reach that digital intermediaries have made available to SMEs. According to International Trade Centre (ITC) "SME Competitiveness Outlook 2018: Business Ecosystems for the Digital Age" (2018), pg. 17, "Platforms have levelled the playing field considerably for SMEs by lowering the barriers to entry and extending to companies of all sizes the advantages of cost and speed that can be gained from trading online." According to a Public First Report "Google's Economic Impact in Europe" (Feb 20), pg. 26 "64% of new European businesses (less than 5 years old) agreed that the costs of starting a business have reduced substantially because of internet tools", and "61% of small businesses (fewer than 250 employees) in Europe agreed that online tools have made it easier for their business to compete with larger enterprises".

As SMEs grow in size, they necessarily learn not to base their entire business model on any particular trading partner or distribution channel (as is the case for all other businesses and industries).

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

To the extent that large online platform companies play a gatekeeper or rule-setting role over their own ecosystems, this is inherent to competition in the market. As acknowledged by the EC's special advisor report on digital competition policy, J. Crémer, Y.-A. de Montjoye, H. Schweitzer "Competition Policy for the Digital Era" (2019), rule-setting by platforms is necessary because, "such rule-setting and 'market design' determine the way in which competition takes place." Ibid., pg. 60. Furthermore, "the fact that platforms choose rules is not a problem per se; we should welcome competition between different business models and different platform architectures and encourage innovation in that space — indeed, these types of innovation have allowed platforms to generate large efficiencies by enabling transactions that were not possible." Ibid., pg. 61. For example, rule-setting can increase trust in an ecosystem, which increases demand and drives new users to adopt new technological solutions that they would not have otherwise done but for the value that the ecosystem provides.

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

Media that has little commercial value now has to compete with an abundance of content suppliers with very low distribution costs. This kind of intense competition may result in some media companies going out of business. To the extent that governments want to subsidise non-competitive media companies because of a greater appreciation for the value that they provide (that is not perceived by consumers), governments should subsidise such media companies directly.

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

> Large online platform companies generate tremendous value for the economy as a whole, and for SMEs in particular. It is not clear that new regulatory rules would increase aggregate consumer surplus.

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

> This depends on the types of prohibitions. Certain conduct by dominant undertakings is likely to cause anticompetitive harm (e.g. tying, exclusivity), but there may still be justifications for such conduct. A blanket prohibition would remove the possibility of such potentially pro-competitive conduct, and the resulting consumer welfare benefits.

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

> Given the multi-sided nature of platforms, an ex-ante assessment of the competitive effects of conduct is prone to type I errors. Any prohibitions should be imposed after a careful case-by-case assessment of the facts at hand, including competitive dynamics, market circumstances, and possible countervailing justifications.

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

> No specific regulatory authority is needed because there is no clear evidence that markets are not functioning efficiently in the interest of consumers.

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

> n/a

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

> n/a

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

> n/a

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

> n/a

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

> Any new rules should have specific, clear, and transparent objectives so as to provide legal certainty for industry.

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

> n/a

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

> Large online media platforms facilitate media pluralism: lowering transaction costs and opening up markets to global competition. We no longer have to rely on a radio station to broadcast our music, a television station to watch videos, a publisher to distribute writing, or a distributor or retailer, to reach customers. Apple, Amazon, Facebook, Google, Netflix, Spotify and other digital media suppliers are predicated on the idea that shelf-space is unlimited and that consumers should have access to as much choice as possible. Such platforms do not have the incentive to limit media pluralism as a diversity of content is complementary and will attract more users to the platform.

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:

- ☐ Institutional cooperation with other authorities addressing related sectors – e.g. competition authorities, data protection authorities, financial services authorities, consumer protection authorities, cyber security, etc.
- ☑ Pan-EU scope
- ☐ Swift and effective cross-border cooperation and assistance across Member States
- ☐ Capacity building within Member States
- ☐ 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

> n/a

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
- ☐ Monitoring powers for the public authority (such as regular reporting)
- ☑ 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

> Yes. The regulatory oversight tools will depend on the type of ex-ante rules being enforced. Any framework should try to preserve market incentives to invest, innovate and compete vigorously on the merits.

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

> There is no clear evidence that markets are not functioning efficiently in the interest of consumers.

27 Are there other points you would like to raise?

3000 character(s) maximum

> n/a

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	n/a	n/a
Private marketplace auctions	n/a	n/a
Programmatic advertising with guaranteed impressions (non-auction based)	n/a	n/a
Behavioural advertising (micro-targeting)	n/a	n/a
Contextual advertising	n/a	n/a
Other	n/a	n/a

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

3000 character(s) maximum

> Technology companies bring more transparency than ever before and continue to increase the level of transparency. Companies provide increasing levels of authentication, verification, sometimes auditing rights, which are subject to agreements with advertisers and publishers. Their incentive is to improve their service, and part of it depends on how it is measured and how effective it is.

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

> n/a

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	n/a	n/a
Private marketplace auctions	n/a	n/a
Programmatic advertising with guaranteed impressions (non-auction based)	n/a	n/a
Behavioural advertising (micro-targeting)	n/a	n/a
Contextual advertising	n/a	n/a
Other	n/a	n/a

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

> CCIA members in the ads ecosystem want to provide advertisers with accurate information and controls that will satisfy their brand safety and marketing needs, as well as better inform their future advertising efforts and spend. CCIA members offer different tools which match their services and offerings.

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

> The digital economy has improved the advertising experience. Thanks to ad-supported business models, consumers enjoy goods and services at a lower price, oftentimes at no cost. Thanks to investments in technology, consumers usually receive relevant advertising to them.
>
> To provide a more personalised online experience, some digital platforms use information that is drawn from users' profiles and/or online activities with proper consent. CCIA members recognise that users want more control and transparency over their online environment, including the advertising that is presented to them. In response, platforms and intermediaries have undertaken efforts to address these concerns and better empower consumers by developing new privacy controls and practices.
>
> It is important to distinguish first-party advertising (display ad) and third-party advertising.

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

> CCIA members do not generally publish or share detailed data on the advertisements published on their platforms, nor the advertiser or viewership rates. The use of any personal data in relation to ads served on the platform will be governed by the relevant platform's terms of service and privacy policy. While there may be legitimate public interest purposes for researchers and other third-parties to gain access to specific sets of data, any sharing of such information must take into account the relevant provisions of current data protection laws, the risks for user privacy and the risk of exposing third-party commercially sensitive data.

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

3000 character(s) maximum

> CCIA members are motivated to maintain trust in the digital advertising ecosystem. Members involved in online advertising have detailed policies against ads for illegal and harmful goods or services, and comply with all applicable laws and regulations. Ads that violate these policies can be blocked on the relevant networks and repeat offenders can have their advertising accounts terminated.

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

> In addition to developing and applying clear rules on the content that can be displayed online by publishers using advertising intermediation services, CCIA members work with industry organisations (e.g., the Interactive Advertising Bureau (IAB)) to tackle issues relating to ad quality, ad fraud and brand safety.

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

3000 character(s) maximum

> CCIA is open to discuss transparency requirements for (automated) content moderation and recommender systems. Many CCIA members already regularly publish transparency reports on their content moderation practices and outcomes. When calling for more transparency, it is important to aim for meaningful transparency pursuing a fair purpose. We do not want to overwhelm consumers, businesses or authorities. CCIA supports proportionate transparency requirements that strike a balance between the need for transparency, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets. Furthermore, any transparency and reporting obligation must adhere to existing EU legislation and fundamental rights. The alleged asymmetries in information, as mentioned in the inception impact assessment, should be assessed taking into account the EU data protection rules, the need for better enforcement of existing tools (GDPR) and the upcoming initiatives such as the data strategy.

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

3000 character(s) maximum

> CCIA members could consider making the following information publicly available: (i) how auctions work, (ii) how contextual ads work, (iii) how other ad models work, (iv) platforms' policies on personalised ads, (v) what caused a particular ad to appear to a particular consumer (e.g., based on contextual, past search history, or purchases, etc), (vi) who is responsible for ads, (vii) what data is being collected by whom and why, and (viii) regular transparency reports on enforcement and on platforms' efforts to maintain a trustworthy ecosystem.

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

3000 character(s) maximum

Transparency measures outlined in question 16, consistently deployed and reported, would go a long way to promoting accountability without the need for audits.

Any audits would need to allow for protecting proprietary and user information, while also not inhibiting innovation by putting new developments at risk/limiting competition.

If an audit proposal is considered, a number of questions regarding the scope of such audits/monitoring would need to be addressed collectively first, such as: (i) Is self-auditing or self-certification possible? (ii) Would cadence be regular or ad hoc? (iii) Would every algorithmic change have to be audited (problematic given the fast pace of innovation in the sector) or only major algorithmic changes? And if the latter, who decides what a major change is? (iv) What authority would control? Would there be a single authority at EU level or would companies work with the relevant national authority? (v) Would the relevant authority have to issue special information requests or be entitled to certain info as a matter of course? (vi) Would auditing be done ex-ante or ex-post? What would it mean in practical terms? (vii) Would platforms have to wait for approval before rolling out innovation/algorithmic changes?

When calling for more transparency, it is important to aim for meaningful transparency pursuing a fair purpose. We do not want to overwhelm consumers, businesses or authorities. CCIA supports proportionate transparency requirements that strike a balance between the need for transparency, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets.

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

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

CCIA members are mindful of the importance of responsible political advertising and have taken a range of approaches to political advertising with varying definitions. Those companies that allow political advertising generally believe that there is merit in discussion of meaningful transparency for consumers to know more details about the political advertising displayed, in order to help promote trust in digital political advertising and confidence in electoral processes.

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

> When calling for more transparency, it is important to aim for meaningful transparency pursuing a fair purpose. CCIA supports proportionate transparency requirements that strike a balance between the need for transparency, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets. We do not want to overwhelm consumers, businesses or authorities.

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

3000 character(s) maximum

> n/a

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?

> Some CCIA member companies offer online intermediation services, which connect service providers that want to transport people, products, goods, or offer some services, with consumers who want to use their services. Each intermediary has its own business model and specific way of operating using a variety of techniques and technologies.
>
> CCIA members offering collaborative economy services are connecting supply and demand, and facilitate the transaction for instance by helping with the payment. The platform does not own the product(s) or service (s) that are subject to the transaction, but invests significantly to create the user interface that facilitates the provision of services. Typically, the platform connects customers and service providers and/or merchants via the digital intermediation service that the platform provides.

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

> It is difficult to generalise companies' operations and business models in light of the very different nature of goods and services offered. Some digital service providers refund/bear the responsibility towards the consumer, while for others the responsibility lies with the actor providing the services (e.g. couriers). There are additionally significant differences depending on the country and local regulations that may be apply.

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

> Collaborative economy platforms have put structural checks and balances as due diligence in place to build trust in their services and on their platforms, and to avoid non-payment.

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

> The contractual relationship varies from one intermediary to another. Companies do not restrict the access to their application, other than the restrictions imposed by national regulations. Service providers are free to choose when, where and if they will work. The service providers have full control of their time, and control the amount of time they wish to spend working on the platform. Some individuals work only a few hours per month, while others are more active. Some service providers may want to finance their studies, while others choose to work full-time.
>
> Furthermore, CCIA members have commercial contracts with their service providers with a non-exclusivity clause, meaning the service providers can use multiple apps or set up their own businesses. Such flexibility is very much valued by service providers, and would in most countries not be feasible in an employment relationship.
>
> One other big benefit of the self-employment model is that it allows creating earning opportunities, especially in sectors where there are no restrictive regulations like delivery. For such activities, for instance, there are no strict requirements for a courier's language skills or educational background, platform work often provides opportunities for those unemployed and underemployed individuals who are having a hard time finding work on the traditional labor market. This is equally true even in more regulated sectors of the collaborative economy such as ride-hailing. For instance, in France, 25% of UberX drivers were unemployed before driving with the Uber app, 43% of which had been unemployed for more than a year.

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

> There are different business models across the collaborative economy that affect price setting.
>
> In some instances, the intermediary service provider, the so-called platform here, is in a privileged position to assess the supply and demand, allowing it to optimize the price to match the benefits for both, the customer and the service provider (e.g. riders/couriers). When setting the price, such platforms take various economic variables into consideration setting the price at a level where there is sufficient customer demand, merchant supply, and courier service supply. This dynamic pricing maximizes efficiencies in the market, benefiting all actors.
>
> In relation to rider/courier services, we would caution against the idea of riders/couriers setting up their own prices, which could lead to a race to the bottom. Generally, there is more supply for courier/rider services than there is demand in the market. Such market dynamics would drive courier/driver earnings down if they would be allowed to freely compete against each-other on price. This became evident in Uber's Californian experience, where prices and financial benefits for the riders/couriers went down. The rides went in practice to the lowest bidder and some drivers ended up earning less than they did under usual rules.

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

> As mentioned, there are different business models across the collaborative economy that affect price setting. In general, the majority of the price by the consumer goes to the service provider and in the case of delivery to the "product maker" (i.e. restaurants) . The "cut" taken by the digital intermediary/the technology provider will also vary depending on many factors such as the market or business realities.

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

3000 character(s) maximum

> As mentioned above, the profile of the service providers varies significantly. The service providers have full control of their time, and control the amount of time they wish to spend working on the platform. They can work a couple of hours a week to full-time. They are free to decide what suits them the most. Companies offer very flexible environments which enable service providers to arrange their work schedule depending on their needs. This independence and flexibility is very much valued by service providers.
>
> For example, in Slovakia nearly half (45%) of Private Hire Vehicle (PHV) drivers spend fewer than 10 hours per week logged in to their apps, while in the UK it's closer to a fifth (22%). This varies across countries and cities and reflects the many different ways in which people choose to use the app.

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

Individuals that provide their service as self-employed, either as business users on platforms or offline, rarely form a clearly defined group or share common interests. This is even more the case with digital intermediaries where business users use platforms for different amounts of time depending on their needs and barriers at the entry.

Platform experience confirms the Commission study ("The future of work? Work of the future!", May 2019) that showed that many service providers do not develop a professional identity as a platform worker. They do not consider the option of common representation as often platform work is used as a tool rather than a standalone employment form by workers, who are often represented through other means in their main employment. Eurofound also pointed this out in its 2019 study "Platform work: Maximising the potential while safeguarding standards?".

Platforms keep innovating and creating mechanisms that are in service of the service providers to express their concerns. On top of that, they engage with service provider associations as well as established labor unions in different countries across the EU while participating in processes that are put in place by national governments regulation like the French Mobility Law which encourages the consultation with business users.

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

Service providers need to submit required permits when they sign up for the platform. We believe that the DSA should clarify and harmonise the obligations of platforms in order to address existing concerns while preserving a dynamic digital single market, and favour the emergence of new players. The current fragmentation is a real challenge for small and medium-sized players, as there are 27 different regimes for the 27 EU Member States, with on top of it, the regional specificities.

The DSA should also remove artificial barriers that currently exist. For instance,
- In Belgium, an Uber ride should have a car valued at minimum €33K.
- In Germany, an Uber rider needs to go back to its parking spot before taking another ride, which is extremely not environmentally friendly.

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

Service providers are free to choose when, where and if they will work. The service providers have full control of their time, and control the amount of time they wish to spend working on the platform. This flexibility allows them to maximize the earning opportunities, using multiple platforms and developing their own business at the same time.

The intermediary set checks and balances in place protecting business users and consumers, from unpleasant experiences (e.g. non-payments). The recently implemented Regulation on fairness and transparency in online platform-to-business relationship ("P2B") provides additional transparency and redress mechanisms to service providers.

Some local regulations constitute barriers to entry, as it oblige service providers to invest a certain amount of resources and time to be able to provide their service. This has a critical impact on service providers' earnings. For instance, some service providers will have to work full-time to compensate for their investment. This could lead to market saturation in supply and demand, resulting in lower earnings per service provider, online or offline.

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

The downside of the self-employment model in general, whether it is online or offline, is that access to social protections is in many countries conditional upon being in an employment relationship. This leaves self-employed service providers facing inequality in social protections compared to employees, as they lack similar effortless access to things like unemployment benefits or sick leave. It is important to keep in mind that this situation is not unique to the platform economy and has existed in other types of independent work long before the emergence of platform work.

Another (related) problem with the uncertainty relating to the legal status of platform work is that platforms are constrained in their ability to provide benefits to their self-employed partners. For example, providing certain types of insurance coverage to service providers increases the risk of jeopardising the flexibility and independence that self-employed people choose and prefer. These issues need an approach that will disconnect the social protection from an employment model and enable the efficient protection of all irrespective of employment status.

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

- Insurance and other benefits: Platforms should be encouraged to offer insurance or other benefits to their self-employed partners. Currently, the legal risk of re-classifying the relationship between a platform and an independent worker prevents intermediaries from increasing their offering, with a focus on education and further protections to their partners in many countries.

- Social protections: Access to social protections should be equal for all workers, regardless of the type of their work – be it employment or self-employment. Independent workers should have access to a social safety net. In order to enable this, policy-makers should incentivise competition among intermediaries on the

basis of the offering of social protection. Platforms compete in order to attract service providers who can offer their services without exclusivity. This competition could improve those safety nets for the self-employed.

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

CCIA members regularly exchange with their customers and service providers. It is crucial for the platforms to have healthy relationships with both parties. Companies are attentive to service providers' claims and, when possible, are trying to accommodate them.

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

3000 character(s) maximum

Platforms have long provided dispute resolution mechanisms. Should these fail to resolve conflicts, service providers always retain their right to initiate legal proceedings.

In parallel, and since July 2020, Article 14 of the EU Regulation on fairness and transparency in online platform-to-business relationship is already creating a framework allowing service providers/business users to be represented by an organisation or an association.

The barriers to collective bargaining are more practical than legal as the situations of self-employed workers and salaried employees' varies on various aspects:
1. Individuals that provide their service as self-employed, either as business users on platforms or offline, rarely form a clearly defined group or share common interests.
2. Service providers use the platforms/digital intermediaries in various manners. They can use one or different platforms for different amounts of time depending on their needs. Some service providers use a digital intermediary for a few hours, while others will work full-time. Some are using different apps, while others are only loyal to one digital intermediary.
3. Services providers prefer to represent themselves with the tools offered by the digital intermediary /platform, instead of having someone representing them.

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	○	○	○	○	○	○

5 Please specify

3000 character(s) maximum

The current system is fragmented, making it difficult for small and medium-sized companies to grow across the EU single market. For instance,
- The product safety framework is specific to each Member State, meaning procedures need to be adapted to each national market.
- There is no EU VAT register, meaning that the VAT needs to be registered in every Member State where goods are stored and delivered.
- National taxation rules differ significantly.
Sometimes the administrative burden of complying with the various national and regional rules is more expensive than the revenue made in those countries.

An important first step would be the enforcement of existing rules. We would welcome further cooperation between the Member States. If the European Commission would like to create a specific oversight body, or extend the mandate of an existing one, we would suggest to clearly outline the type of body, areas to cover, and mission statement. In both cases, CCIA and its members would like to cooperate with the Member States' authorities or the governing body who will implement the Digital Services Act.

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

7 Please specify the grounds on which these measures were taken (e.g. sale of illegal goods on your service, obligations related to tackling disinformation) and what was your experience?

3000 character(s) maximum

Some CCIA members have been subject to measures from another EU Member State than the one they are established in, when they have been approached by consumer protection authorities.

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

9 Please explain

3000 character(s) maximum

CCIA members comply with the local and national rules of the markets where they operate.

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

As mentioned above, the current system is fragmented, making it difficult for small and medium-sized companies to grow across the single market. For instance, in product safety, VAT harmonisation, or cross-border parcel delivery services. Sometimes the administrative burden of complying with the various national and regional rules is more expensive than the revenue made in those countries.

Enforcing the existing rules is key to success. We would welcome further cooperation between the Member States. If the European Commission would like to create a specific oversight body, or extend the mandate of an existing one, we would suggest to clearly outline the type of body, areas to cover, and mission statement. In both cases, CCIA and its members would like to cooperate with the Member States' authorities or the governing body who will implement the Digital Services Act.

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

12 Please explain

3000 character(s) maximum

The turnover wouldn't be the right figure to look at to get a sense of companies' financial health. Some turnover went up, but the associated cost to COVID-19 went also up, meaning the overall profit went down.

The impact across the EU varies depending on the regions, and services offered. For instance,
Some online marketplaces fulfilment centres had to close, or remained open but at a high financial cost to comply with the security measures.
Content hosting platforms had to increase their effort to detect illegal and harmful content (e.g. sale of counterfeits, unsafe products, fake news, disinformation).
The ride-hailing services saw their activity draw drastically.

Several CCIA members took a vast array of measures including: automated, and where necessary, human monitoring of the content displayed in relation to various keywords and a categorisation of products at risk of scams. Price gouges are addressed by algorithms and general preventive measures are taken to ensure traders are properly informed of possible unfair practices. CCIA members took firm temporary bans on the selling or advertising of specific products such as masks or alcoholic gels, they listed only the confirmed and reputable providers of certain products. In addition, many of our members launched consumer and seller information campaigns in line with official expertise and governmental advice about COVID-19. The number of products/offers/ads withdrawn are very significant, up to one million in a week, on the biggest operator, with hundreds of thousands of price gouges detected. CCIA members have set dedicated teams to address

the crisis and evolution of practices and are proactively, including on a 24/7 basis, monitoring developments on their platforms with regular sweeps.

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

Recent weeks have proven how valuable digital services are for Europeans' wellbeing. Children study through online tools, social networks keep families connected, people work remotely and consumers stream newly released content like movies.

In 2018, 83% of Europeans used the internet at least weekly and about 76% daily or almost every day, compared with 81% and 72% respectively a year earlier. EU citizens engage in a broad range of online activities: they order goods or services online (69%), participate in social networks (65%), use online banking (64%) or watch video on-demand (31%).

Small and medium-sized enterprises (SMEs), as well as micro-businesses, are also hugely benefiting and growing thanks to digital services providers. For instance, 18% of business turnover in the EU comes from e-sales. Moreover, 26.2% of European enterprises purchase cloud computing services and incorporate cloud technologies for improving operations while reducing costs, representing an increase of 25% compared to 2016.

CCIA supports the European Commission's desire to improve the Single Market for services through addressing fragmentation and gaps left in the framework. Digitalisation is a great opportunity for many European SMEs to get in touch with consumers not only from their national market, but across the EU.

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 believe that there is some room for improvement for the cooperation 1° between Member States, but also 2° between the authorities of the same countries (e.g.: Consumer, Data and Competition Authorities).

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

If the European Commission would like to create a specific oversight body, or extend the mandate of an existing one, we would suggest to clearly outline the type of body, areas to cover, and mission statement. It is essential that this body is aligned with the national entities and does not contradict opinions/decisions made by national authorities as it would create confusion and legal uncertainty.

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

3000 character(s) maximum

Enforcement is key to the success of the Digital Services Act. The tech industry would welcome transparency reports or information that promotes good governance and participation, but also protects the legitimate interests of users, business users and intermediaries.

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

Any authority involved in supervising online platforms should have a strong evidence base, an in-depth understanding of the relevant markets, and quantitative and qualitative skills relevant to the applicable regulatory toolkit.

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

Yes, CCIA supports the European Commission's objective to treat all digital services equally, regardless of where they are established.

CCIA supports the proportionate and targeted approach suggested by the European Commission. We wouldn't be opposed in principle to creating specific graduated categories for different platform types, that reflect the nature of the service provided and the degree of knowledge and control that the service has over individual items of content, in order to decrease fragmentation between the Member States. However, we strongly oppose defining a category of responsibility based on the size of market power. The risk of such an approach could be to incentivise successful players to stay small in the EU to avoid regulation. Another unintended consequence would be fragmentation and the migration of illegal content, goods or conduct to smaller, less regulated platforms (including those not established in the EU). We strongly support the Commission's notion of removing "disincentives for their voluntary actions to address illegal content, goods or services they intermediate."

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

We would encourage the EU to develop strong cooperation with non-EU supervisors, and set agreements with countries where many online platforms/intermediaries are coming from (e.g.: China, United States).

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

Beneficial cooperation and coordination between national regulators requires that such regulators have clear mandates and harmonised regulatory objectives. Such cooperation needs to be transparent in order to support industry and stakeholder confidence. Regulators should also be subject to clear rules on any reuse or sharing of information, and must subject to a system of judicial review. In addition, the interaction between national legal systems needs to be considered where cross-border cooperation is in operation.

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

As mentioned above, stronger cooperation among national bodies, but also among the Member States' entities, is needed especially when it comes to consumer protection, VAT, taxation or parcel delivery. The EU is particularly well placed to incentivise such cooperation among the Member States, and bring a harmonised approach.

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

> While it is rather early to assess the effectiveness of ERGA's new role in the cooperation mechanism in cross-border cases, we welcome the opportunity that exists within ERGA for national regulators to exchange best practices and experiences regarding the regulatory framework. Such exchanges enable the promotion of consistency in the approaches taken within Member States, and support the expression of the country of original principle.

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	★★★★★ (5)
Agreeing on guidance for consistent implementation of rules under the AVMSD	★★★☆☆ (3)
Ensuring consistency in cross-border application of the rules on the promotion of European works	☆☆☆☆☆ (0)
Facilitating coordination in the area of disinformation	★★★☆☆ (3)
Other areas of cooperation	☆☆☆☆☆ (0)

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

Enforcing the existing rules is key to success. We would welcome further cooperation between the Member States. If the European Commission would like to create a specific oversight body, or extend the mandate of an existing one, we would suggest to clearly outline the type of body, areas to cover, and mission statement. In both cases, CCIA and its members would like to cooperate with the Member States' authorities or the governing body who will implement the Digital Services Act.

The EU has already adopted frameworks to deal with problematic content, goods or conduct online. Before adding another layer, and potentially creating confusion, we would urge legislators to wait for the implementation of these frameworks. The Copyright Directive, goods package, VAT reforms, consumer omnibus Directive and changes at UPU-level to fees, as well as the Terrorist Content Regulation, are major changes that have not yet come into force. Their impact must be understood to assess any further gaps and proportionate responses, including within the existing voluntary frameworks.

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