FACEBOOK

September 8, 2020

FACEBOOK RESPONSE TO EC PUBLIC CONSULTATION ON THE DIGITAL SERVICES ACT (DSA)

About you

1 Language of my contribution

- ❑ Bulgarian
- ❑ Croatian
- ❑ Czech
- ❑ Danish
- ❑ Dutch
- ❑ **X 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
- ❑ **X Company/business organisation**
- ❑ Consumer organisation
- ❑ EU citizen
- ❑ Environmental organisation
- ❑ Non-EU citizen
- ❑ Non-governmental organisation (NGO)
- ❑ Public authority
- ❑ Trade union
- ❑ Other

3 First name

Anna

4 Surname

Helseth

5 Email (this won't be published)

ahelseth@fb.com

6 Scope

- ❑ **X International**
- ❑ Local
- ❑ National
- ❑ Regional

7 Organisation name

Facebook

8 Organisation size

- ❑ Micro (1 to 9 employees)
- ❑ Small (10 to 49 employees)
- ❑ Medium (50 to 249 employees)
- ❑ **X Large (250 or more)**

9 What is the annual turnover of your company?

- ❑ <=2m EUR
- ❑ <=10m EUR
- ❑ <= 50m EUR
- ❑ **X More than 50 m EUR**

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

- ❑ Yes
- ❑ **X No**

11 Would you describe your company as :

- ❑ a startup?
- ❑ a scaleup?
- ❑ **X a conglomerate offering a wide range of services online?**

12 Is your organisation:

- ❑ **X 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

- ❑ **X 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

n/a

15 When was your organisation first established?

February 2004

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?

- ❑ **X 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
- ❑ **X Ireland**
- ❑ Italy
- ❑ Latvia
- ❑ Lithuania
- ❑ Luxembourg
- ❑ Malta
- ❑ Netherlands
- ❑ Poland
- ❑ Portugal
- ❑ Romania
- ❑ Slovak Republic
- ❑ Slovenia
- ❑ Spain
- ❑ Sweden

20 Transparency register number:

28666427835-74

21 Country of origin

- ❑ 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
- ❑ Egypt
- ❑ Macau
- ❑ San Marino
- ❑ Andorra
- ❑ El Salvador
- ❑ Madagascar
- ❑ São Tomé and Príncipe
- ❑ Angola
- ❑ Equatorial Guinea
- ❑ Malawi
- ❑ Saudi Arabia
- ❑ Anguilla
- ❑ Eritrea
- ❑ Malaysia
- ❑ Senegal
- ❑ Antarctica
- ❑ Estonia

- ❑ Maldives
- ❑ Serbia
- ❑ Antigua and Barbuda
- ❑ Eswatini
- ❑ Mali
- ❑ Seychelles
- ❑ Argentina
- ❑ Ethiopia
- ❑ Malta
- ❑ Sierra Leone
- ❑ Armenia
- ❑ Falkland Islands
- ❑ Marshall Islands
- ❑ Singapore
- ❑ Aruba
- ❑ Faroe Islands
- ❑ Martinique
- ❑ Sint Maarten
- ❑ Australia
- ❑ Fiji
- ❑ Mauritania
- ❑ Slovakia
- ❑ Austria
- ❑ Finland
- ❑ Mauritius
- ❑ Slovenia
- ❑ Azerbaijan
- ❑ France
- ❑ Mayotte
- ❑ Solomon
- ❑ Islands
- ❑ Bahamas
- ❑ French
- ❑ Guiana
- ❑ Mexico
- ❑ Somalia
- ❑ Bahrain
- ❑ French

- ❑ Polynesia
- ❑ Micronesia
- ❑ South
- ❑ Africa
- ❑ Bangladesh
- ❑ French
- ❑ Southern and Antarctic Lands
- ❑ Moldova
- ❑ South Georgia and the South Sandwich Islands
- ❑ Barbados
- ❑ Gabon
- ❑ Monaco
- ❑ South Korea
- ❑ Belarus
- ❑ Georgia
- ❑ Mongolia
- ❑ South Sudan
- ❑ Belgium
- ❑ Germany
- ❑ Montenegro
- ❑ Spain
- ❑ Belize
- ❑ Ghana
- ❑ Montserrat
- ❑ Sri Lanka
- ❑ Benin
- ❑ Gibraltar
- ❑ Morocco
- ❑ Sudan
- ❑ Bermuda
- ❑ Greece
- ❑ Mozambique
- ❑ Suriname
- ❑ Bhutan
- ❑ Greenland
- ❑ Myanmar/Burma
- ❑ Svalbard and Jan Mayen
- ❑ Bolivia

- ❑ Grenada
- ❑ Namibia
- ❑ Sweden
- ❑ Bonaire
- ❑ Saint
- ❑ Eustatius and Saba
- ❑ Guadeloupe
- ❑ Nauru
- ❑ Switzerland
- ❑ Bosnia and Herzegovina
- ❑ Guam
- ❑ Nepal
- ❑ Syria
- ❑ Botswana
- ❑ Guatemala
- ❑ Netherlands
- ❑ Taiwan
- ❑ Bouvet Island
- ❑ Guernsey
- ❑ New Caledonia
- ❑ Tajikistan
- ❑ Brazil
- ❑ Guinea
- ❑ New Zealand
- ❑ Tanzania
- ❑ British Indian Ocean Territory
- ❑ Guinea-Bissau
- ❑ Nicaragua
- ❑ Thailand
- ❑ British Virgin
- ❑ Islands
- ❑ Guyana
- ❑ Niger
- ❑ The Gambia
- ❑ Brunei
- ❑ Haiti
- ❑ Nigeria
- ❑ Timor-Leste

- ❑ Bulgaria
- ❑ Heard Island and McDonald
- ❑ Islands
- ❑ Niue Togo
- ❑ Burkina Faso
- ❑ Honduras
- ❑ Norfolk Island
- ❑ Tokelau
- ❑ Burundi
- ❑ Hong Kong
- ❑ Northern Mariana Islands
- ❑ Tonga
- ❑ Cambodia
- ❑ Hungary
- ❑ North Korea
- ❑ Trinidad and Tobago
- ❑ Cameroon
- ❑ Iceland
- ❑ North
- ❑ Macedonia
- ❑ Tunisia
- ❑ Canada
- ❑ India
- ❑ Norway
- ❑ Turkey
- ❑ Cape
- ❑ Verde
- ❑ Indonesia
- ❑ Oman
- ❑ Turkmenistan
- ❑ Cayman
- ❑ Islands
- ❑ Iran
- ❑ Pakistan
- ❑ Turks and Caicos Islands
- ❑ Central African Republic
- ❑ Iraq
- ❑ Palau

- ❑ Tuvalu
- ❑ Chad
- ❑ Ireland
- ❑ Palestine
- ❑ Uganda
- ❑ Chile
- ❑ Isle of Man
- ❑ Panama Ukraine
- ❑ China
- ❑ Israel
- ❑ Papua
- ❑ New Guinea
- ❑ United Arab Emirates
- ❑ Christmas Island
- ❑ Italy
- ❑ Paraguay
- ❑ United Kingdom
- ❑ Clipperton
- ❑ Jamaica
- ❑ Peru
- ❑ **X 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.
- **X Public**
  - Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

- ❑ **X 23. I agree with the personal data protection provisions**

SAFETY AND RESPONSIBILITY

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

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

- ❑ **X A notice-and-action system for users to report illegal activities**
- ❑ **X A dedicated channel through which authorities report illegal activities**
- ❑ **X Cooperation with trusted organisations who report illegal activities, following a fast-track assessment of the notification**
- ❑ A system for the identification of professional users ('know your customer')
- ❑ **X A system for sanctioning users who are repeat infringers**
- ❑ A system for informing consumers that they have purchased an illegal good, once you become aware of this
- ❑ **X Multi-lingual moderation teams**

- ❑ Automated systems for detecting illegal activities. Please specify the detection system and the type of illegal content it is used for
- ❑ **X Other systems. Please specify in the text box below**
- ❑ No system in place

2 **Please explain.**
5000 character(s) maximum

Facebook is committed to making its service a safe and respectful place for all users to share and connect with others. Keeping people safe is one of Facebook's core principles and one which it takes very seriously. This commitment begins with the Terms of Service, which all users must accept and which prohibits users from doing or sharing anything that is unlawful, misleading, or fraudulent or that infringes or breaches someone else's rights.

In addition to our Terms, we also have our Community Standards, the global set of policies that outlines what is and is not allowed on Facebook. Our Community Standards are publicly available on our website and apply to everyone, all around the world, and to all types of content. Given the global and diverse nature of the community we serve, our Community Standards do not necessarily reflect any specific legal system, nor are they intended to cover all local laws. However, as they are designed to prevent harm, they do overlap in a number of instances with local law.

Our Community Standards are enforced both reactively based on reports from the community, as well as proactively. People can and do report content to us that they believe violates our Community Standards, including Pages, groups, profiles, individual posts and comments, using the dedicated tools on the platform. We process millions of Community Standards reports every week, and the vast majority of reports are reviewed within 24 hours. To do this, we use a combination of human review and automation. If reported content is found to violate our Community Standards, we take it down; if it doesn't, we leave it up. We also provide appeal channels where appropriate.

Facebook also takes additional action against people who seriously or repeatedly violate our policies. For example, we will terminate the accounts of repeat intellectual property infringers where appropriate and may impose additional restrictions against repeat or blatant infringers.

Supplementing our Terms and Community Standards are our policies that govern specific types of content or activity on Facebook. For example, paid ads are subject to our Advertising Policies, and Commerce content, like Marketplace listings, is subject to our Commerce Policies. Both types of content are subject to review prior to running, primarily using automated tools to detect likely violations of these policies, supplemented and aided by

human reviewers where appropriate. People can also report such content that they believe violates our policies. If we detect a violation of our policies, we will reject the content.

Since our policies are developed for a global user base and are independent from local legal requirements, we have **separate reporting mechanisms for our users to report content they believe violates the law.** These legal reporting channels available include:

- **Intellectual property reporting channels** — We provide reporting forms for intellectual property rights holders to report content they believe violates their rights, including copyright infringement, trademark infringement and counterfeits, as well as an email address for reporting at ip@fb.com. (Our Intellectual Property policies are also reflected in the Community Standards.)
- **Defamation reporting form** — This form allows parties to report content they believe is defamatory under local law.
- **Legal removal request form** — This form allows parties in European Union Member States to report content they believe violates local laws.
- **NetzDG reporting form** — This form allows parties in Germany to report content they believe violates one or more of the German Criminal Code provisions set forth in NetzDG.

Facebook has multiple operations teams in offices throughout the world that handle reports through these channels. Together, they represent a global team of trained professionals who provide around-the-clock coverage every day of the year in multiple languages, including English, major European languages, and a number of others. These specially trained teams work closely with Facebook's in-house lawyers, and where needed external lawyers, to assess and act on reports of illegal content.

Facebook also takes additional action against people who seriously or repeatedly violate our policies. For example, we will terminate the accounts of repeat intellectual property infringers where appropriate and may impose additional restrictions against repeat or blatant infringers. We also invest building tools to help rights holders remove potentially infringing content, such as our specialized Commerce & Ads IP Tool and have further invested in technology such as artificial intelligence and machine learning to remove or limit the visibility of potentially infringing content, independent of any rights holder's report. All of this work is based on close collaboration with rights holders, a key example of which is our joining of the European Commission's Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet.

3 **What issues have you encountered in operating these systems?**
5000 character(s) maximum

Our systems--both automated and human--are built and intended to detect and enforce against violations of our applicable policies. However, our systems are not able to detect all possible policy violations. We face particular challenges with respect to:

- *Context*: When review requires understanding of the context surrounding the content at issue, automated systems are particularly challenging. Indeed, there are many signals and characteristics of a piece of content that may, in isolation or on their face, appear benign, or where context indicates whether a particular piece of content violates policy. One example is hate speech, where automated measures cannot necessarily distinguish between a hateful term and condemnation of that term.
- *Local law*: As noted, our Community Standards do not, and are not intended to, reflect any particular local legal regime. And as local law varies from Member State to Member State, our systems cannot necessarily capture the nuance of local law. For example, personal rights violations are particularly challenging, as these violations often require additional information (such as the truth or falsity of allegedly defamatory remarks) which we often do not have and, as an online intermediary, cannot be expected to have.
- *False positives*: Just as automated systems may not capture all policy violations, so too are they prone to over-enforce and result in the removal of legitimate free speech.
- *Accuracy of reports*: We have also found that the accuracy of user reports of policy violations is highly variable across type and country .
- *Abusive, fraudulent and overreaching reports*: In some contexts, we have faced challenges in addressing abusive, fraudulent or otherwise overreaching reports, such as legal reports in the intellectual property space, where legal bases are cited to support a takedown request of perfectly legitimate content.
- *Adversarial bad actors*: These difficulties are in some instances compounded by bad actors that intentionally circumvent our detection systems.

Given these challenges, our measures to tackle policy-violating content -- in particular our automated measures -- are not, and cannot be, perfect. We therefore continue to rely on stakeholders to report such content using our various reporting channels.

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

- ❑ Yes
- ❑ **X 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.**

We continue investing in keeping our users safe across our platform. Currently, over 35 000 people work for users' safety and security at Facebook. We have not estimated the costs of our notice-and-takedown systems or other measures to remove policy-violating or illegal content from the service, but as the above-described measures illustrate, Facebook takes these commitments very seriously and invests heavily in the people and tools needed to take the measures outlined in this consultation's response. While we have not estimated the cost of building and maintaining these tools, each entailed the commitment of significant time and resources to develop from the ground up — and we have continued to devote significant resources to scaling and improving these important tools, taking into account feedback from third parties.

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.**

As explained, our Community Standards are developed for a global user base and although in many instances they are designed to prevent harm that may naturally overlap with the objectives of local laws, they operate independently of local legal requirements. In addition, Facebook provides separate reporting mechanisms for its community of users, government authorities and intellectual property rights holders to report content that they believe violates relevant local laws. To capture both sides of this content enforcement, Facebook publishes regular reports to give our community visibility into how we enforce policies, respond to data requests and protect intellectual property, while monitoring dynamics that limit access to Facebook products for example triggered by local law reporting.

1. Community Standards Enforcement Report - This report shares metrics on how we are doing at preventing and taking action on content that goes against our Community Standards. These actions may include removing content or covering content with a warning screen. Content violating Community Standards is not necessarily illegal. Our latest Community Standards Enforcement Report was published in August 2020 and covers the period between April and June 2020. During this time, Facebook removed millions of pieces of content. For example, we actioned 22.5 million pieces of content violating our hate speech policy and 8.7 million pieces of terrorist content.
2. Content Restrictions Based on Local Law - When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability in the country where it is alleged to be illegal. We receive reports from governments and courts, as well from non-

government entities such as members of the Facebook community and NGOs. This report details instances where we limited access to content based on local law.

3. Intellectual Property Report - This report outlines our IP practices, the volume and types of IP reports we receive from rights holders, and how much content those reports affect. The categories covered are copyright infringement, trademark infringement, and counterfeits. Our most recent IP Transparency Report reflects that in the period July-December 2019, Facebook removed more than 2.7 million pieces of content in response to more than 487,000 IP reports.
4. NetzDG Transparency Report - The Network Enforcement Act (NetzDG) requires social networks receiving more than 100 complaints per calendar year to publish a half-yearly transparency report about NetzDG complaints. This report provides information about how we handle illegal content on our platform, and details specific figures on NetzDG complaints and how we handled such complaints.

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

Facebook has multiple lines of defence against behaviour that is consistent with or indicative of "suspicious behaviour." The first line is Facebook's terms and policies. Facebook's Terms of Service prohibit users from using Facebook's products to do or share anything that is unlawful, misleading, discriminatory, or fraudulent. They also inform users that Facebook employs dedicated teams around the world and develops advanced technical systems to detect misuse of its products, harmful conduct towards others, and situations where Facebook may be able to help support or protect its community.

Examples of Facebook's efforts in this area include:

- Enforcing on our policies, including those that may overlap with potentially illegal behaviour (e.g., sale of non-medical drugs); removing content when we become aware of it; enforcing against accounts for severe or repeat offences; and developing and deploying proactive, automated tools to detect such content.
- Bringing greater transparency to ads to increase accountability for advertisers and help prevent abuse; and detection and enforcement in respect of policy-violating ads.
- Detecting and removing fake accounts and combatting Coordinated Inauthentic Behaviour (CIB).
- Limiting the spread of spam and other misleading and deceptive tactics designed to increase viewership.
- Violence, harm, threat to safety. We also aim to prevent potential offline harm that

may be related to content on Facebook. While we understand that people commonly express disdain or disagreement by threatening or calling for violence in non-serious ways, we remove language that incites or facilitates serious violence. We remove such content, disable accounts, and we also try to consider the language and context in order to distinguish casual statements from content that constitutes a credible threat to public or personal safety. In determining whether a threat is credible, we may also consider additional information like a person's public visibility and the risks to their physical safety.

From a transparency and accountability perspective, as mentioned, Facebook publishes a Community Standards Enforcement Report (CSER), which contains sections dedicated to reporting on fake accounts, spam, and certain regulated goods, as well as an IP Transparency Report and a transparency report under Germany's NetzDG law. As part of its transparency reporting, Facebook also publishes a report on Government Requests for User Data to provide information on the nature and extent of these requests and the strict policies and processes it has in place to handle them.

Please see also our answer to Section B, Question 3.

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

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

- ❑ **X Spread of political disinformation in election periods?**
- ❑ **X Other types of coordinated disinformation e.g. in health crisis?**
- ❑ **X Harmful content for children?**
- ❑ **X Online grooming, bullying?**
- ❑ **X Harmful content for other vulnerable persons?**
- ❑ **X Content which is harmful to women?**
- ❑ **X Hatred, violence and insults (other than illegal hate speech)?**
- ❑ **X Other activities which are not illegal per se but could be considered harmful?**

2 **Please explain your policy.**
5000 character(s) maximum

All users must accept Facebook's Terms of Service as a condition of using the Facebook service. The Terms prohibit users from doing or sharing anything that is unlawful, misleading, or fraudulent or that infringes or breaches someone else's rights.. By accepting the Terms,

users also agree that they may not do anything that breaches Facebook's terms or policies, including the Community Standards, which are global sets of policies that outline what is and is not allowed on Facebook.

Our Community Standards cover a wide range of objectionable or harmful content, including – of relevance to this question in particular – content that:

- Promotes violent behaviour
- Threatens the safety of others
- Is considered hate speech
- Is considered graphic violence
- Is considered spam
- Is harmful to minors

Our Community Standards apply to everyone, all around the world, and to all types of content.
They are based on feedback from our community and the advice of experts in fields such as technology, public safety and human rights.

To help ensure that everyone's voice is valued, we take great care to craft policies that are inclusive of different views and beliefs, in particular those of people and communities that might otherwise be overlooked or marginalised. These views are brought together in a meeting we typically hold every two weeks to discuss new policies or amendments to existing policies – called the Content Policy Forum (previously referred to as the Content Standards Forum).

In addition to the Community Standards, we have additional policies that apply to different product areas and experiences. For example, our Advertising Policies apply to paid ads on Facebook and Instagram. Our Commerce Policies apply to use of our Commerce tools and products, like Marketplace. These policies apply in addition to--not instead of--the Community Standards and cover a wide range of areas including some of the areas listed above. As with the Community Standards, these policies are global in nature and do not--and are not intended to--displace local legal requirements. All users are required to comply with the law when using our products, and our on-platform policies further govern the behaviour of users on our platforms. For a more fulsome list of various terms and policies, please refer to section 5 of our Terms of Service.

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

3000 character(s) maximum

People can and do report content to us that they believe violates our Community Standards and other policies, including Pages, groups, profiles, individual posts, comments and marketplace content, using the dedicated tools on the platform. We process millions of these reports every week, and the vast majority of reports are reviewed within 24 hours[1]. To do this, we use a combination of human review and automation. If reported content is found to violate our Community Standards or other policies, we take it down; if it doesn't, we leave it up.

Users can also report paid ads that they believe violate our policies via Facebook's online reporting tools. If the reported ad is determined to violate our policies, the ad is removed, and the advertiser receives a standardized, automated message informing them of the removal.

Child exploitation reporting

We make it easy for people to report violations of our policy, and we prioritize reports of child sexual exploitation. People can report instances of child exploitation content using the reporting flow available on our site. Our teams are trained to recognise this content and pass it to our team of child safety experts. More than 35,000 people work on security and safety at Facebook, including specially trained teams with backgrounds in law enforcement, online safety, analytics, and forensic investigations, who review and report to the National Center for Missing and Exploited Children (NCMEC), in accordance with U.S. law.
In turn, NCMEC works with law enforcement agencies around the world to help victims.

When we become aware of newly generated CEI based on reports or otherwise, the content is hashed to prevent further sharing, reported to NCMEC, and deleted. As is always the case, if we have reason to believe a child is in immediate/imminent danger, we may proactively refer a case to local law enforcement (as well as report it to NCMEC), to make sure the child is immediately safeguarded.

Bullying of minors prevention

- **Reporting.** We make it easy to report bullying content, and we also give our users tools so that they can self-resolve issues and seek additional support from a trusted friend or a specialized local NGO. In addition, people can appeal any bullying or harassment decision we make. Depending on the seriousness of the situation, a person suffering from bullying can opt to:

[1] Subject to certain constraints due to COVID pandemic, more information https://about.fb.com/news/2020/08/community-standards-enforcement-report-aug-2020/

    - Unfriend or Unfollow the person.
    - Block the person.
    - Report the person or any abusive content they have posted.
        - In addition, if people see a friend or family member being bullied or harassed, now they can anonymously report on their behalf by clicking on the menu above the post that they are concerned about.

- **Comment Moderation Tools:** we introduced a way for people to hide or delete multiple comments at once from the options menu of their post. We launched filters allowing people to filter out potentially bullying comments or create a customized keyword filter to block certain comments.

Suicide prevention

Suicide prevention tools have been available on Facebook for more than 10 years and were developed in collaboration with mental health organisations such as Save.org, National Suicide Prevention Lifeline, Forefront and Crisis Text Line, and with input from people who have personal experience thinking about or attempting suicide. We further updated those tools in 2015 and in 2016 we expanded the availability of the tools globally — with the help of over 70 partners around the world — and improved how they work based on new technology and feedback from the community.

On Facebook if someone posts something that makes you concerned about their well-being, you can reach out to them directly and also report the post to us. We have teams working around the world, 24/7, who review reports that come in and prioritize the most serious reports like suicide. We provide people who have expressed suicidal thoughts with a number of support options — to reach out to a friend, contact a helpline, or see tips. In serious cases, when it's determined that there may be imminent danger of self harm, Facebook may contact local authorities.

Misinformation

We have a three-step approach to misinformation: **Remove, Reduce** and **Inform**.This means that we **remove** from the platform any content that is found to violate our Community Standards. In addition, we remove fake accounts as well as accounts engaged in coordinated inauthentic behaviour (please find here a report about the networks we recently removed), and that amounts to cybersecurity threats. We also remove harmful misinformation, that is to say misinformation that can lead to imminent physical harm, and this is the existing policy we are applying to certain pieces of **COVID-19 misinformation** since January 2020. We

remove paid ads that have been determined to be misinformation, in accordance with our Misinformation Advertising Policy.

Secondly, we **reduce** the distribution of content in users' feed that has been debunked by our third-party fact-checking partners.

Finally, we create products to **inform** users with additional and contextual information so they can decide what to read, trust, and share, such as by including links on debunked content to articles written by fact-checkers, and asking users to reconsider sharing content that has already been fact-checked and determined to be misinformation. We are also encouraging our community to have a critical view of what they see online and support media and digital literacy initiatives.

4 **What other actions do you take? Please explain for each type of behaviour considered.**
5000 character(s) maximum

Facebook employs a broad range of actions to keep abuse off its service and products beyond the important enforcement actions we take in response to user reports. As our Community Standards Enforcement Report shows, our technology to detect violating content is improving and playing a larger role in content review. Our technology helps us in three main areas: proactive detection, automation and prioritisation. These three aspects of technology have transformed our content review process and greatly improved our ability to moderate content at scale. However, there are still areas where it's critical for people to review. For example, discerning if someone is the target of bullying can be extremely nuanced and contextual. In addition, AI relies on a large amount of training data from reviews done by our teams in order to identify meaningful patterns of behavior and find potentially violating content. That's why our content review system needs both people and technology to be successful.

When we remove content for violating our policies, we may also take action against the user who has posted that content. That action may include temporary restrictions, warnings, down-ranking, prohibiting the user from participating in ad-related functions, or removal of the user from our platform. We also take a range of measures to detect and enforce against policy-violating content before it is reported to us so that we do not have to rely solely on reports to address such content.

We take actions to support **critical counterspeech** initiatives by enforcing strong content policies and working alongside local communities, policymakers, experts, and changemakers to unleash Counterspeech initiatives across the globe. We support a number of initiatives that build on empowering people and challenging hateful and extremist narratives (P2P Facebook Global Challenge, Online Civil Courage Initiative), and we actively participate in the Global Internet Forum to Counter Terrorism (GIFCT).

We want Facebook to be a place where **women feel empowered** to communicate. Facebook regularly partners with women's safety organisations to ensure our products and services protect survivors of domestic violence, sexual assault, and stalking. For example, we have collaborated with The National Network to End Domestic Violence (NNEDV) in the U.S., to offer tips to survivors of abuse so that they can use Facebook to stay connected with friends and family, while controlling their safety and privacy to prevent further abuse. Facebook also has a zero tolerance policy when it comes to facilitating sex trafficking. Sexual slavery is a pressing and terrible global problem. We remove content that threatens or promotes sexual violence or exploitation.

5 **Please quantify, to the extent possible, the costs related to such measures.**
5000 character(s) maximum

We continue investing in keeping our users safe across our platform. Currently, over 35 000 people work for users' safety and security at Facebook. Please see also our answer to Section A, Question 5.

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

- ❑ **X Yes**
- ❑ No

7 **Please explain.**
3000 character(s) maximum

Keeping young people safe online has been a top priority for Facebook.

We have no tolerance for the sexual exploitation of children on Facebook, and we use cutting-edge technology to proactively and aggressively remove it. We have specially trained teams with backgrounds in law enforcement, online safety, analytics, and forensic investigations, which review content and report to the National Center for Missing and Exploited Children

(NCMEC), in accordance with U.S. law. In turn, NCMEC works with law enforcement agencies around the world to find and help victims. We also work with external experts, including the Facebook Safety Advisory Board and our Global Safety Network of over 400 safety experts, to discuss and improve our policies and enforcement around online safety issues, especially with regard to children.

We do not allow child sexual exploitation, abuse and nudity, and we require people to connect on Facebook using their authentic identity so that we can create a safe environment where people know with whom they are connecting and can trust and hold one another accountable.

Technology is our business and we use it to fight child sexual exploitation, both to help us prioritize the most serious reports and to proactively find content and remove it. We have been using photo-matching technology since 2011 to thwart the sharing of known child sexual imagery on our platform. We also use artificial intelligence and machine learning to proactively detect child nudity and previously unknown child exploitative content. We're also using technology to find accounts that engage in potentially inappropriate interactions with children on Facebook so that we can remove them and prevent additional harm.

In August 2019, we announced we are open-sourcing two technologies that detect identical and nearly identical photos and videos, so our industry partners, smaller developers and nonprofits can use them to more easily identify abusive content and share hashes — or digital fingerprints — of different types of harmful content.

We also work with our expert partners to collect lists of external sites known for hosting child sexual exploitation material and block access to those sites from our platform.

- We use a URL list maintained by the Internet Watch Foundation for webpages where images and videos of child sexual abuse have been found to help prevent accessing those URLs from our platform.
- We also prevent type-aheads for searches containing known child exploitation terms, utilising resources like Thorn's Keyword Hub list of known CSAM seeking terms, and display a pop-up warning when people attempt searches with these terms.

We also do not tolerate bullying on Facebook because we want the members of our community to feel safe and respected. We will remove content that purposefully targets private individuals with the intention of degrading or shaming them. We recognise that bullying can be especially harmful to minors, and our policies provide heightened protection for minors because they are more vulnerable and susceptible to online bullying.

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?**

- ❑ **X Yes**
- ❑ No

2 **What action do you take when a user disputes the removal of their good or content or service, or restrictions on their account? Is the content/good reinstated?**
5000 character(s) maximum

People can and do report content to us that they believe violates our Community Standards, including Pages, groups, profiles, individual posts and comments, using the dedicated tools on the platform

Any system that operates at scale and for a global user base will make errors. For this reason, in April 2018, we launched **appeals**, globally, for content that was removed for violating our Community Standards for nudity or sexual activity, hate speech and violence. We've extended this option so that re-review is now available for additional content areas, including dangerous organisations and individuals (which includes our policies on terrorist propaganda), bullying and harassment, regulated goods, and spam.

We are continuing to roll out re-review for additional types of Community Standards violations, but there are some violation types – for example, severe safety policy violations – for which we don't offer re-review. We are also beginning to provide appeals not just for content that we took action on, but also for content that was reported but not acted on.

Here's how the process works for many of our **appeals**:

- If your photo, video or post has been removed for violating our Community Standards, you will be given the option to “Request Review” on both mobile and desktop.
- Appeals are reviewed by our Community Operations team in most cases within 24 hours.
- If we've made a mistake, the content will be restored and we will notify the person who requested the appeal.
- When an appeal happens, it is usually sent to our Community Operations team for a second review by someone different than the person who originally reviewed the content.

As noted, advertisements and Commerce listings are subject to both reactive and proactive review under our Advertising Policies and Commerce Commerce Policies, respectively, and

content that violates these policies will be rejected. For both paid ads and Commerce, we offer the option to appeal these rejections. Advertisers also have the option of editing their ad and resubmitting.

Separately, when content is removed based on an intellectual property report, the reported user is provided the reason for the removal as well as the rights holder that reported the content. If the user believes the content should not have been removed, they may reach out to the reporting party directly to resolve the matter. In the case of copyright and trademark removals, users also are provided an opportunity to appeal to Facebook directly. If the appeal is meritorious, the content will be restored.

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

Our automated systems have been trained on hundreds of thousands, if not millions, of different examples of violating content and common attacks. As we're improving our technology, we are looking to optimise its precision.

One way to optimise this is using what we learn during the content review process. In particular, the appeals mechanism is very important to help us improve our machine learning systems. Appeals from users help us reduce the amount of false positives (by training our systems) and increase the precision of our automated systems.

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

- ❑ **X Yes**
- ❑ No

5 **Please explain.**
5000 character(s) maximum

We have created an independent review body called the "Oversight Board." This board will help Facebook answer some of the most difficult questions around freedom of expression online: what to take down, what to leave up and why. The board will use its independent judgment to support people's right to free expression and ensure that those rights are being adequately respected. The board's decisions to uphold or reverse Facebook's content

decisions will be binding, meaning that Facebook will have to implement them, unless doing so could violate the law.

When fully staffed, the board will consist of 40 members from around the world that represent a diverse set of disciplines and backgrounds. These members will be empowered to select content cases for review and to uphold or reverse Facebook's content decisions. The board is not designed to be a simple extension of Facebook's existing content review process. Rather, it will review a selected number of highly emblematic cases and determine if decisions were made in accordance with Facebook's stated values and policies. These decisions will be publicly available for everyone to see.

In addition to rendering binding decisions, the board will be able to recommend changes to Facebook's content policies through official "policy advisory statements." In accordance with the Oversight Board's bylaws, Facebook must consider the board's recommendation and publicly disclose whether we took action in accordance with the recommendation.

D. Transparency and cooperation

1 **Do you actively provide the following information (multiple choice):**

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

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

- ❑ **X Yes**
- ❑ No

3 **Do the reports include information on:**

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

4 **Please explain.**
5000 character(s) maximum

Facebook publishes regular transparency and enforcement reports to lend greater visibility into how Facebook enforces its policies, responds to legal and data requests, and protects intellectual property. As set forth in response to Question 6 of Part A, these include:

- Legal Requests Report
- IP Transparency Report
- Community Standards Enforcement Report (CSER)
- NetzDG Transparency Report

Facebook is constantly refining its processes and methodologies in order to provide the most meaningful and accurate numbers on how it is enforcing its policies. This includes implementing internal information quality processes that create further checks and balances in order to make sure it is sharing valid and consistent metrics. Facebook also seeks external input to ensure its methods are transparent and based on sound principles.

Data Transparency Advisory Group

One example of Facebook's efforts to seek out analysis and input from subject matter experts outside of Facebook is its work with the Data Transparency Advisory Group (DTAG), an external group of international academic experts in measurement, statistics, criminology, and governance. In May 2019, DTAG provided its independent public assessment of whether the metrics Facebook shares in the CSER provide accurate and meaningful measures of how Facebook enforces its policies, as well as challenges Facebook faces in this work, and what Facebook does to address them. Overall, DTAG found Facebook's metrics to be reasonable ways of measuring violations and in line with best practices. DTAG also provided some recommendations for how Facebook can continue to be more transparent about its work, which Facebook continues to implement and explore.

Product Policy Forum

Another way Facebook seeks to ensure transparency of its operations is by involving external stakeholders in the Product Policy forum. This meeting brings together a cross-functional and geographically diverse group from across the company and beyond to discuss new policies and suggested changes to existing policies. Facebook also involves a large number of external organisations, such as academia, NGOs, law enforcement and policymakers, who help Facebook ensure that its policies land in the right place. Summaries from each meeting are posted publicly on Facebook's Newsroom site.

5 **What information is available about 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

Facebook Newsroom & Facebook for Business

Facebook consistently updates the public on how it uses new technological measures or harnesses existing automated tools in a new way to combat a wide variety of policy-violating content by posting updates to the Facebook Newsroom.

For example, Facebook has posted about how it has been able to supplement its efforts to proactively detect child nudity and previously unknown child exploitative content by using artificial intelligence and machine learning, including how it uses media matching technology, to proactively detect child exploitation material and, in some cases, prevent it from ever being uploaded (please see response to Question 3 of Part B for more information on these technologies). Indeed, Facebook has published posts in its Newsroom extensively on how it uses artificial intelligence, machine learning, and computer vision to find terrorist organisations and content, hate speech, pornography, and violence.

Facebook has also explained in the Newsroom how it aims to use artificial intelligence to reduce misleading ads by identifying and capturing cloaked websites, and that automated tools can help Facebook determine whether someone is creating fake accounts in mass from one location and block certain IP addresses altogether so that those bad actors can't access Facebook's services to create fake accounts.

Facebook also uses the Newsroom to share news of new pilot programmes, such as a pilot programme launched last year to help potential victims of non-consensual sharing of intimate images from appearing on Facebook and Instagram without their consent.

We have also published information about various integrity measures on our Facebook for Business site, including our Good Questions, Real Answers blog. For example, we released a blog post and detailed site dedicated to explaining the measures we take to tackle counterfeits on Facebook. The blog post is available at https://www.facebook.com/business/news/good-questions-real-answers-how-facebook-helps-brands-protect-against-counterfeits and the anti-counterfeiting site is available at https://www.facebook.com/business/tools/anti-counterfeiting/guide.

Facebook Engineering

Facebook publishes detailed information about its automated tools and technologies at Facebook Engineering, an online resource center dedicated to exploring Facebook's latest projects in AI, data infrastructure, development tools, virtual reality, and more. For example, Facebook posted about the large-scale machine learning system it built and deployed called Rosetta, which has been widely adopted by various product teams within Facebook and

Instagram and used, for example, to automatically identify content that violates Facebook's hate speech policy in various languages.

Facebook AI

Facebook describes the types of artificial intelligence tools it is exploring on its Facebook AI page, including natural language processing, reinforcement learning, and speech and audio tools. For example, Facebook describes how it is combatting COVID-19 misinformation and predatory content by using computer vision classifiers and local feature-based instance matching. These automated tools help Facebook enforce its temporary ban of ads and commerce listings for medical facemasks and other products, proactively take action against manipulated media at scale, and put warning labels on millions of pieces of content based on their independent fact-checking partners.

6 **How can data related to your digital service be accessed by third parties and under what conditions?**

- ❑ **X Contractual conditions**
- ❑ Special partnerships
- ❑ **X Available APIs (application programming interfaces) for data access**
- ❑ **X Reported, aggregated information through reports**
- ❑ **X Portability at the request of users towards a different service**
- ❑ **X 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

Facebook shares data and insights in a variety of ways adhering to applicable data protection and privacy rules. We provide data to researchers and partner organisations and have established data products for partnerships in the areas of health, elections, disaster relief, and connectivity.

Our business tools provide owners of Facebook Pages with aggregated information on user engagement with their Pages. This information allows businesses to measure and improve their commercial presence and performance, which makes their partnership with us more valuable.

Beyond this, the primary way that parties obtain access to certain data that users choose to share with third parties is via APIs. The Facebook Platform enables developers to build innovative and unique products and solutions, empowering them to grow their businesses. We are committed to building a safer, more sustainable platform to create trust with users and drive long term value for developers. Thus, safeguarding and protecting user data is a shared responsibility we have with all developers on the platform. As part of our commitment to user privacy, we have shared our vision for empowering developers to act as stewards of the platform. More here.

Not all API tools provide the same level of access. In order to access data beyond what is in a user's public profile, a developer must go through several steps: (1) a developer must identify the permissions they would like to access and request that access to us, (2) the user must provide consent to that access, and (3) the developer's application must then call on the Facebook API only as needed, retrieving data based on the user's discretion. The developer must also agree to our Facebook Business Tool terms (facebook.com/legal/technology_terms). The overarching purpose of these terms is to protect our users and their data and to ensure a common minimum standard of quality for all features and functions that Facebook users may see and experience.

For portability, since the entry into force of the GDPR, we have seen an increased interest in users exercising their 'right to data portability'. This is noted through an increased interest in our "Download Your Information" tool. This tool provides users with access to their Facebook information, as well as some observed and inferred data. The "Download Your Information" tool allows users to request to download a single data file in HTML or JSON format, which can then be uploaded to a new provider. Together with others in the industry, we are working on an initiative based on the "Data Transfer Project" that will enable users to transfer all of their photos or videos to a new provider in a one-off transfer. This transfer can be repeated at the user's initiation.

With regard to publishing reports, we regularly publish reports through our transparency portal (transparency.facebook.com) to give stakeholders visibility into community standards enforcement, government access requests, and internet disruptions. These reports are published at regular intervals and we seek to provide users with as much information as possible while taking into consideration our legal constraints.

2. Clarifying responsibilities for online platforms and other digital services

1 **What responsibilities should be legally required from online platforms and under what conditions?**

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

	Yes, by all online platforms, according to the activities they intermediate (e.g. content hosting, selling goods or services)	Yes, only by larger online platforms	Yes, only platforms at particular risk of exposure to illegal activities by their users	Such measures should not be legally required
Maintain an effective 'notice and action' system for reporting illegal goods or content	X			
Maintain a system for assessing the risk of exposure to illegal goods or content				X
Have content moderation teams, appropriately trained and resourced	X			

Systematically respond to requests from law enforcement authorities				X
Cooperate with national authorities and law enforcement, in accordance with clear procedures				X
Cooperate with trusted organisations with proven expertise who can report illegal activities for fast analysis ('trusted flaggers')				X
Detect illegal content, goods or services				X
In particular where they intermediate sales of goods or services, inform their professional users about their obligations under EU law				X

Request professional users to identify themselves clearly ('know your customer' policy)				X
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)				X
Inform consumers when they become aware of product recalls or sales of illegal goods				X
Cooperate with other online platforms				X

for exchanging best practices, sharing information or tools to tackle illegal activities				
Be transparent about their content policies, measures and their effects	X			
Maintain an effective 'counter-notice' system for users whose goods or content is removed to dispute erroneous decisions	X			
Other. Please specify				

2 **Please elaborate, if you wish to further explain your choices.**
5000 character(s) maximum

While Facebook supports regulation requiring digital platforms to have systems in place to address content that is unlawful, a homogenous one-size-fits-all approach is not a viable solution. Obligations should be proportionate in relation to the nature and characteristics of the service, and include appropriate safeguards to protect the privacy of users in the course of legitimate and lawful activities, and any requirements should be tailored to the variety of business models involved and developed in collaboration with stakeholders. Any regulation must take this into account. For example, small and medium-sized online platforms and services may have less capability and resources, and less advanced processes than larger

companies. Nevertheless, small and medium-sized companies can have higher risks of exposure to illegal and/or harmful activities conducted by their users.

Facebook also believes that online platforms should be required to be transparent about their content policies, measures, and their effects. However, there is a limit to what online platforms can (and should) publicly disclose about their enforcement measures. Bad actors are constantly evolving their tactics, and limiting the amount of specific and technical information that is publicly known about these technologies reduces the risk that these individuals find new ways around or means to manipulate existing technologies.

Certain responsibilities are already addressed in existing regulations, which are better suited for those purposes. In our view, requests from law enforcement authorities to online platforms, in so far as they relate to data disclosure, should be governed by the EU e-Evidence Regulation, which sets harmonized EU rules and upholds a high standard of protection to fundamental rights, and the applicable laws of the jurisdiction in which the relevant data controller is located. We also believe that obligations to cooperate with national authorities and law enforcement must respect international human rights, including the core principles of freedom of expression and privacy.

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

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

4 **Please explain**
3000 character(s) maximum

Maintaining a notice-and-takedown regime for clearly unlawful content is desirable and necessary to protect freedom of expression and information. Because hosts cannot feasibly monitor their entire platforms, and because they do not have (and cannot be expected to have) all of the information and context necessary to independently assess the legality of every one of the billions of pieces of content they host, a notice-and-takedown regime is necessary to avoid extreme overblocking of fully legitimate and desired content (which would otherwise be a host's only alternative).

Facebook has put in place mechanisms to receive and address legal requests, including dedicated reporting forms for users to submit requests, in order to streamline and facilitate the expeditious processing of their requests.

In order to facilitate the expeditious removal of illegal content through these channels, a notification should contain all the necessary information for the recipient to act without communicating further with the sender. It might be desirable to establish the minimum information needed for a notice to be actionable, for example:

- Name and contact information of the reporting party, so that a platform may communicate with them during the review process, request additional information if needed, etc.;
- His or her relationship with the report and/or reported content (e.g., an individual reporting content on his/her own behalf; an attorney on behalf of his/her client; the rights holder);
- URL(s) to clearly identify each piece of content the user is reporting so that a platform knows precisely what to review;
- An explanation of why the user believes the content is clearly unlawful, including identification of the specific law(s) he or she believes the content violates;
- Supporting evidence to demonstrate why the reporter believes the content is clearly unlawful (e.g., documents or information demonstrating the falsity of a statement in the case of defamation, or information showing a rights holder's registered trademarks for a counterfeit report); and
- Whether the user has obtained a court order establishing the unlawfulness of the reported content.

Such criteria should also be technology-neutral to accommodate the diversity of digital services. For example, a notification for an app store might not work for an online marketplace. Such notification systems should be accessible to all actors and easy to use.

All notifications should be made in good faith and, where the allegations of unlawfulness relate to a private cause of action, should be made by the aggrieved party with standing to bring that claim. For example, intellectual property reports should be submitted only by rights holders or their authorized representatives, as those are the parties who will have the knowledge and legal basis to submit a valid claim of infringement. Similarly, any claim of defamation should be submitted only by the party whose rights have been allegedly violated. Those who are proven to persistently abuse "notice-and-takedown" procedures by sending claims which have no legal basis should be held accountable, and intermediaries should be

permitted to ignore their notices on the grounds that such notices do not convey "actual knowledge".

5 **How should the reappearance of illegal content, goods or services be addressed, in your view? What approaches are effective and proportionate?**
5000 character(s) maximum

Particularly in the area of content regulation, how online intermediaries handle the reappearance of illegal content raises critical questions for fundamental rights such as freedom of expression and information, which also must be considered in the face of technical and legal realities. First, context is critical. An "identical" post may be unlawful if repeated in the same context, but may be entirely lawful and protected speech if repeated in a different context (including by a different person) – for example, if denouncing the unlawful content. Images, videos and text can be used in different contexts that must be evaluated independently. Failing to account for context could result in the removal of content that is entirely legitimate and in violation of free expression principles. Facebook's automated tools for detection and removal have progressed significantly, but they nevertheless are not an appropriate vehicle for prevention of the reappearance of content, for both practical and technical reasons. First, automation is necessarily unable to interpret the context associated with a particular piece of content, nor is it designed or suited for determinations of violations of local law, which can differ among Member States. Determining a post's message is often complicated, requiring complex assessments by human reviewers around intent and an understanding of how certain words are being used. Relying on automated tools alone to identify identical or "equivalent" content may well result in the removal of perfectly legitimate and legal speech. Second, automated tools are far from perfect, and identifying similar and/or equivalent content becomes virtually impossible, particularly where reappearing content has been slightly altered or, as noted, presented in a different context.

Moreover, imposing legal requirements, whether by judicial decision or legislation, regarding such content would run afoul of Article 15 of the ECommerce Directive and also would raise serious sovereignty and international comity concerns. As discussed further below in response to Section II Question 6, Article 15's prohibition against general monitoring obligations is of vital importance to the proper functioning of the intermediary liability regime and to the appropriate safeguarding of freedom of expression and other fundamental rights. Not only would a requirement to prevent the reappearance of content be such a general monitoring obligation, as it would require platforms to proactively search and/or scan every piece of content at the moment of upload, but a piece of content that was removed as illegal in one jurisdiction might not be illegal if it were to reappear and be reported in another jurisdiction. For example, content deemed defamatory in the Netherlands may not be unlawful in Austria, and outcomes further differ across Member States if the content involves

a public figure. If Member States do not agree on whether content is unlawful, then Facebook—a private company and intermediary—cannot and should not be required to make this determination preemptively simply because the content was previously determined to be unlawful in one country.

An effective and proportionate response should take the above considerations into account. 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.

6 **Where automated tools are used for detection of illegal content, goods or services, what opportunities and risks does their use represent as regards different types of illegal activities and the specificities of the different types of tools?**
3000 character(s) maximum

We do not generally use automated tools to detect illegal content, goods, or services; rather, we use automated tools, like machine learning classifiers, to detect and enforce against some forms of harmful content that violate our policies. We recognise that in some instances, such content may also be unlawful in particular jurisdictions.

Classifiers are systems we train to identify signals or patterns in content which suggest it might violate one of our policies – such as our policies on nudity or violence – based on violating content we have removed in the past. When these systems detect potentially violating content, they may remove the posts automatically or send it to be reviewed by our teams of content reviewers in order to make a final determination.

For a number of years, we have also been using media matching technology to detect photos or videos which are identical or nearly identical to materials we have already removed for violating our policies on matters like child nudity, sexual exploitation of children, and terrorism. For example, if we previously removed a terrorist propaganda video from a terrorist organisation, we can use media matching technology to automatically detect it if re-uploaded. In many cases, this means that this content intended for upload to Facebook simply never reaches other users on the platform.

While we are pleased with this progress, we are conscious that these technologies are far from perfect and can't yet handle complex integrity challenges on their own. While some categories of illegal content may be easier for these systems to identify, many categories of illegal content are by their very nature more nuanced and complex (e.g., hate speech,

personal rights violations like defamation, and IP infringement). These problems are compounded by the fact that different jurisdictions have different standards for what constitutes a legal violation (such as hate speech), and technology simply is not suited to capture the nuances of local law. That's why we also have people, including content reviewers and local law experts, as part of the process to help make these complex decisions.

Illegal content also poses particular enforcement challenges that technology alone cannot solve because bad actors are motivated to evade technologies put in place to detect the illegal content that they share.

Finally, because of the limitations of technology discussed above, greater reliance on automation could pose the risk of over-blocking and erroneous removal of **legal** content, which can have a chilling effect on free expression or violate other fundamental rights and due process. This is why we continue to rely on our community of users and other stakeholders to report content using our robust notice-and-takedown programmes.

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?

Facebook supports a broader European ecosystem in which a variety of stakeholders collaborate to make the online world a safer place. Facebook's collaboration with safety organisations, law enforcement, brands, academics and subject matter experts, trusted partners, and other companies through industry cooperative efforts has proven successful at helping keep people safe and preventing abuse on the internet.

In this regard, we encourage forums for voluntary cooperation such as EC Memorandum of Understanding on Counterfeiting and the EU Internet Forum. Models for intergovernmental cooperation, particularly with non-EU bodies, should also be encouraged as a method to reduce the prevalence of illegal and harmful content on the internet.

We also think it is important to recognise that certain types of cross-border and cross-platform coordinated illegal behaviour is best addressed and led by law enforcement authorities rather than online platforms. These authorities have access to offline information, investigative tools, and legal fact-finding that platforms simply do not have. In these cases, robust intergovernmental cooperation, combined with reporting relationships with various online platforms (see our response to Question 2, Part 2 above), should be encouraged.

8 **What would be appropriate and proportionate measures that digital services acting as online intermediaries, other than online platforms, should 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

Rules appropriate for one type of service may not be appropriate for others. Any legislation should recognise this and allow flexibility for different types of services to address illegal content in a way that is best suited for those services' offerings and technical capabilities rather than requiring uniform measures across platforms.

9 **What should be 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

Illegal activity online is a broad societal concern that requires complex and multifaceted solutions by online and offline stakeholders. Facebook believes that governments, civil societies, and industries are crucial to the fight against illegal activities online and encourages them to take a greater role. Facebook sees two main ways to do this. First, government, civil society, and industries should take an active role in developing baselines for due process and transparency linked to human rights principles and independent regulatory oversight and enforcement (*e.g.*, clear/accessible terms, user reporting/safety tools, adequate resourcing, appeals, user resources/educational materials) that could then be applied across platforms. An independent regulatory body (existing or new) could oversee platforms and assess their codes to encourage a harmonised and transparent approach to combating online illegal activities aimed at protecting users rather than punishing individual instances of bad content.

Second, governments, civil society, and industry bodies could play a leading role in receiving and investigating reports of certain types of illegal content from the public. These entities typically have access to the relevant facts, can conduct legal investigations, and can seek adjudication (or in some cases have authority to determine on their own) as to whether the content is illegal. Once a determination of illegality has been made, these entities could report the content to the relevant online platform for action. These entities should be encouraged to create user-friendly reporting mechanisms, efficient investigative and adjudicative processes, and effective partnerships with online platforms to address illegal activities online.

With respect to intellectual property infringement, rights holders are the only parties that know the extent of their rights and whether specific content constitutes an infringement. Therefore, any enforcement for IP reasons is highly dependent on rights holders' involvement, collaboration and cooperation.

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

Platforms have implemented their own policies, such as our Community Standards, which explain what's allowed on our platforms. These policies may follow local laws, but may also go beyond those laws to address content considered harmful, but not illegal. Harmful content is contextual, difficult to define, often culturally subjective and legally ambiguous in some cases. Therefore, harmful content should therefore not form part of the liability regime.

At the same time, it is desirable for society that online intermediaries have the capacity to moderate lawful but potentially harmful content. In essence, Facebook believes that intermediaries should be responsible for putting systems in place for the removal of specific categories of harmful content. Driving up standards of the systems employed by the operators is likely to result in greater progress than penalising them for individual failures to remove reported content that is harmful but not illegal. Any systematic regulation should not be so prescriptive as to set the processes for the platform.

Should the regulation foresee a regulator to oversee rights and obligations of platforms, the regulator should not be empowered to review decisions made by intermediaries in relation to individual pieces of content, and regulatory sanctions would be appropriate only in the case of systemic failure. As the purpose of regulation is to bring good outcomes, it is typically not helpful to set up regulatory bodies that exclusively have fining power (without the option to issue guidance - binding or non-binding or offer the ability to remedy - instead of fines, or as a first step). Such failure would be assessed through a legal and principle based approach set by the legislator. Safeguards would need to be included for all parties. The regulatory model would then be driven by a focus on best practice - not simply compliance. Therefore, incentives for investment in best practice systems should be a key feature.

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

5000 character(s) maximum

We believe it would be appropriate and proportionate for online platforms to:

- establish and enforce appropriate policies related to minors (their access to the platform, their access to certain types of content or surfaces on the platform); and
- develop reasonable product features to help support compliance with such policies, for example age-gating tools.

Keeping young people safe online is and has been a top priority for Facebook. In addition to our specific measures to protect minors from harmful content and user reporting around harms like bullying, suicide prevention and child exploitation, Facebook uses a number of robust measures to verify age and ensure minors have an age-appropriate experience across Facebook's family of apps.

No age verification mechanism can achieve 100% accuracy; there will always be ways to circumvent even the most robust measures. For our part, Facebook undertakes a series of steps to prevent users under 13 from signing up for Facebook services and detect underage users.

Facebook requires everyone to be at least 13 years old before they can create an account (in some jurisdictions, this age limit may be higher). It violates our Terms of Service to provide a false age when creating an account. Under GDPR, in some EU countries on Facebook, 13 to 15 year olds see a less personalized version of Facebook with restricted sharing and less relevant ads until they get permission from a parent or guardian to use all aspects of Facebook. In addition, when reviewing reports for other potential violations, if our reviewers have reason to believe the account might belong to someone under the age of 13 they are instructed to checkpoint that account and seek verification of age from the account holder.

In addition to ensuring users meet our minimum age requirements, we also have a variety of measures in place to ensure that young people who use our services have age-appropriate experiences. Minors generally have a more limited experience on Facebook when it comes to the features they have access to, who they share and connect with, and the content they see (including ads). Age verification is a complex and industry-wide challenge requiring thoughtful solutions that protect children's safety and privacy without unduly restricting their ability to access information, express themselves, and build community online. Any solution which aims to protect young people online needs to be aware that millions of people often don't have a way to prove their age or identity. Even those who can prove their age or identity would be asked to provide far more detailed personal data than would otherwise be required to use certain services.

It is important to recognise that the steps outlined above are one part of a multi-dimensional approach we take to ensure young people have safe and privacy-protective experiences, and should be assessed jointly with the safety and privacy by design measures we have in place:

- We prevent minors from receiving messages from strangers and we protect sensitive information such as minors' contact info, school or birthday appearing to a public audience.
- Messages sent to minors from adults who are not friends (or friends of the minor's friends) are filtered out of the minor's inbox.
- Additionally, we take steps to remind minors that they should only accept friend requests from people they know.
- Location sharing is off by default. When either an adult or minor turns on location sharing, we include a consistent indicator as a reminder that they're sharing their location.

New minor users are automatically defaulted to share with 'friends' only and their default audience options for posts do not include "public."

- If a minor wants to share publicly, the first time they go to do so they must go to their settings to enable the option and we remind them about the meaning of posting publicly.

The issue of age verification should not be considered in isolation or viewed as a cure-all to the question of protecting children online, but viewed as one of many responses that comprise a holistic approach to the protection of minors online.

We welcome the opportunity to work with the government, civil society and others in industry on alternative solutions.

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 (very necessary).**

	1 (not at all necessary)	2	3 (neutral)	4	5 (very necessary)	I don't know / No answer
Transparently inform consumers					5	

about political advertising and sponsored content, in particular during electoral periods						
Provide users with tools to flag disinformation online and establishing transparent procedures for dealing with users' complaints					5	
Tackle the use of fake-accounts, fake engagements, bots and inauthentic users behaviour aimed at amplifying					5	

false or misleading narratives						
Transparency tools and secure access to platforms' data for trusted researchers in order to monitor inappropriate behaviours and better understand the impact of disinformation and the policies designed to counter it						Please see Q17, Section IV, for our views on transparency reports and auditing of platforms. Please see section II Q 18 with regard to access for trusted researchers.
Transparency tools and secure access to platforms' data for authorities in order to monitor inappropriate behaviours and better						Please see Q17, Section IV, for our views on transparency reports and auditing of platforms.

understand the impact of disinformation and the policies designed to counter i						
Adapted risk assessments and mitigation strategies undertaken by online platforms					5	
Ensure effective access and visibility of a variety of authentic and professional journalistic sources					5	
Auditing systems over platforms' actions and risk assessments						See Q17, Section IV, for our views on transparency reports and

24 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 manipulation and amplification of disinformation.						auditing of platforms.
Other, please specify						

13 **In special cases, where crises emerge and involve systemic threats to society, such as a health pandemic, and fast-spread of illegal and harmful activities online, what are, in your view, the appropriate cooperation mechanisms between digital services and authorities?**
3000 character(s) maximum

There are various ways to ensure successful and timely cooperation between digital services and authorities at times of crisis.

First of all, for crises with imminent risks to people's lives (e.g. terrorist attack), having dedicated protocols in place, such as the Global Internet Forum to Counter Terrorism (GIFCT)'s Content Incident Protocol, has proven extremely effective, like during the Halle shooting. In order to properly respond to these kinds of incidents, however, industry collaboration - as effective as it can be - is not enough to contain the risks. For this reason we supported the creation of the EU Crisis Protocol, seeking a common approach from industry and Member States in addressing the online dimension of terrorist attacks.

For other kinds of crises, with less imminent risks, we support establishing or using existing dedicated channels for authorities to report illegal and harmful content and activities. The use of such channels triggers prioritization of those reports which results in speedier action from the platforms and - consequently- guarantees a better containment of the spread of certain kinds of content.

Facebook has several reporting channels available for government authorities to request takedowns of content that violates our policies or local laws, but also to report cyber/info security issues, information operations, disinformation, suspicious activities, and other potential platform abuses or threats. Facebook also provides a dedicated Trusted Partners channel for key international and non-governmental organisations to submit high quality reports, and a legal removal request form for EU users to report content that they believe violates local laws.

We also underpin the importance of transparent communication between authorities and platforms (within the confines of GDPR). In particular, in a situation of crisis, platforms can be required to provide regular reports on how their systems are performing in terms of moderation and enforcement of crisis- specific content. During the COVID19 outbreak, Facebook regularly reported data to the European Commission about its measures to combat deceptive and exploitative conduct such as disinformation and rogue trading.

With regards to regulators, transparency from their end can be achieved through clearly reasoned removal requests and making data about action taken on harmful content publicly available.

Another good example is cooperation between authorities and online platforms aimed at connecting people to accurate and authoritative information in order to stop misinformation and harmful content from spreading, as shown by Facebook's work with the WHO and other health authorities during the COVID19 emergency.

Experience demonstrates the importance of smooth cooperation among public authorities and online platforms. Having in place clear, structured systems or "protocols" - that include the elements highlighted above - to be activated in time of need will increase our ability to work together and respond efficiently to future challenges.

14 **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 (very necessary).**

	1 (not at all necessary)	2	3 (neutral)	4	5 (very necessary)	I don't know / No answer
High standards of transparency on their terms of service and removal decisions					5	
Diligence in assessing the content notified to them for removal or					5	

blocking						
Maintaining an effective complaint and redress mechanism					5	
Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended					5	
High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting,					5	

removing or demoting content or suspending users' accounts						
Enabling third party insight – e.g. by academics – of main content moderation systems					5	
Other. Please specify						

15 **Please explain.**
3000 character(s) maximum

Facebook supports the idea of an updated EU regulatory framework for online content that ensures companies are making decisions about online speech in a way that minimizes harm but also respects the fundamental right to free expression. As outlined in our White Paper, we consider that regulation should seek to balance these often conflicting issues and aim to properly safeguard freedom of expression by establishing procedural accountability for platforms. In order to do so, regulation should include requirements for companies to publish their content standards and create mechanisms to report violations of these standards..

Facebook is transparent about its Community Standards, the global set of policies that outlines what is and is not allowed on Facebook and is publicly available on our website. Our Community Standards apply to everyone, all around the world, and to all types of content. They are based on feedback from our community and the advice of experts in fields such as technology, public safety and human rights, collected in various forms, including via our

Product Policy Forum, a meeting that typically is held every two weeks to discuss new policies or amendments to existing policies. Summaries from these meetings can be consulted publicly.

It is also 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.

Facebook already shares regular transparency and enforcement reports, such as the Community Standards enforcement report[2] detailing how much content we remove for violating certain of our policies, how much of that content was detected proactively by our automated tools, how much content was appealed when people believed we had made a mistake, and how many of those appeals were successful. Additionally, we regularly publish another report that includes metrics on the number and nature of legal requests we receive from governments and other entities around the world – including requests for data and requests to restrict access to content which they believe violates local law. In addition, Facebook also publishes an IP transparency report, which sets out the number of copyright, trademark and counterfeit reports we receive, the number of pieces of content removed based on those reports, and the overall action rate.

Given the dynamic nature and scale of online speech and the different expectations of users of their experience online, any system operating at scale and for a global user base will be imperfect. For this reason, in order to safeguard freedom of expression, it is essential for platforms to be transparent about its decisions and have appropriate redress mechanisms. Facebook provides feedback and updates to users that report content and informs users whose content has been removed. Additionally, we give users the possibility to appeal our decisions regarding certain content that we took action on and certain content that was reported but not acted on. We offer re-review for many types of violations, except in cases with extreme safety concerns.

16 **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

[2] If a piece of content is reported to us by local authorities because of a potential violation of the local law and it also violates our Community Standards and is subsequently removed, this metric will be included in the CSER_report

When regulating content, careful consideration of the impact on the protection of fundamental rights is of absolute importance and we support including relevant safeguards in any EU content regulation initiative. This is even more so when regulation is aimed at harmful but not illegal content. Additionally, intermediaries should be free to provide any lawful service they develop. These services should not be subject to any a priori licensing regimes or approval schemes for launching or changing certain types of legitimate services.

In order to protect freedom of expression and the other rights highlighted in this question but also privacy, the objective of regulation should be to achieve the essential balance between those rights and users' safety online. Harmonizing definitions, recognising the differences between illegal and harmful content, confirming the e-Commerce Directive's limited liability regime and ban of general monitoring obligations and realising a systemic and proportionate approach to the oversight of online platforms are all important to achieve that balance.

Achieving the right balance is challenging but it's something that Facebook is committed to doing. We want Facebook to be a place where people feel safe but also empowered to express and be themselves. That's why our global set of policies, called Community Standards, are designed to be as comprehensive as possible, to reflect the fact that they serve an incredibly large and diverse community. Words mean different things or affect people differently depending on their local community, language or background. We recognise that and work hard to account for these nuances and apply our policies consistently and fairly to all our users.

Our commitment to expression is paramount, but we recognise that the Internet creates new and increased opportunities for abuse. For these reasons, when we limit expression as a consequence of the application of our policies, we do it in service of a series of values such as:

- authenticity: we believe authenticity creates a better environment for sharing; for this reason, we require people using Facebook not to misrepresent who they are or what they're doing;
- safety: in order to ensure that Facebook is a safe space, expression that threatens people has the potential to intimidate, exclude or silence others isn't allowed;
- privacy: protection of privacy gives people the freedom to be themselves and to choose how and when to share on Facebook and to connect more easily; and
- dignity: we believe that all people are equal in dignity and rights and we expect our users to respect the dignity of others and not harass or degrade others.

In order to protect users, their rights but also their experience online, enforcing against content published online is important but preventing certain behaviours is also paramount.

We believe that the EU regulatory framework for online content should recognise it and include measures aimed at incentivizing positive preventative behaviours and measures.

Facebook invests heavily in prevention, such as by funding academic research into different kinds of harmful behaviours and supporting NGOs initiatives in the space of counterspeech. We are also encouraging positive interaction on our platforms through technology, such as - for instance - on the Facebook app we introduced the context button, which lets people know when they are about to share a news article that is more than 90 days old, but allows them to continue to share if they decide the article is still relevant.

Another way that Facebook has worked to balance questions of fundamental rights and safety on the platform is with the recent creation of the Oversight Board. The Oversight Board was created to help us answer some of the most difficult questions around freedom of expression online: what to take down, what to leave up, and why, in accordance with our Community Standards. The Board will use its independent judgment to support people's right to free expression and ensure those rights are being adequately respected. Its decisions will be binding, meaning Facebook will have to implement them, unless doing so would violate the law.
Facebook remains open to the Oversight Board becoming a voluntary cross-industry body in the future and the governing documents of the Oversight Board have been written in such a way to allow for contributions by other companies in the future.

Facebook has also submitted itself to a unique Civil Rights audit in the US, aimed at strengthening and advancing civil rights on our service. This audit has been a deep analysis of how we can strengthen and advance civil rights at every level of our company. As a direct response to feedback received through this exercise, we have begun making changes in several areas, including strengthening our policies and enforcement against harmful content, fighting against discrimination in ads and protecting elections. However, what has become increasingly clear is that this is the beginning of the journey and that we have a long way to go.

17 **In your view, what information should online platforms make available in relation to their policy and measures taken with regards to content and goods offered by their users? Please elaborate, with regards 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

Facebook's Terms of Service clearly state that people may not use our products to do or share anything that is unlawful, misleading, discriminatory or fraudulent, or that infringes or violates someone else's rights. Facebook also has developed a comprehensive set of Community Standards that outline what is and is not allowed on Facebook. The goal of having such policies in place is to create a safe environment, whilst respecting freedom of expression. However because of fragmentation with regard to what is illegal (as this can be different in different Member States), and because we are often not privy to the necessary information off-platform to determine if elements would constitute illegal content, combined with the global nature and scale of our services, there can be challenges in the distinction between harmful but legal versus illegal content.

As referenced in our response in Section A, Question 2, there are a number of separate reporting mechanisms for users to report content that they believe violates the law.

Within the Help Center there are dedicated information pages for intellectual property rights holders, legal removal requests and defamation reporting forms.

Facebook also has other dedicated channels for, e.g., governments (Government Casework Channel), trusted flaggers, consumer and advertising authorities (The Consumer Policy Channel for reports related to commercial content or activity on the platform) and law enforcement (Law Enforcement Online (Data) Requests).

Our framework is such that our policies may be viewed as stricter than the laws in one country but would be compatible with regards to what is considered illegal in the laws of another country. For this reason, when Facebook receives a report via one of its legal reporting channels[3], we generally first assess if the content violates our Community Standards or other policies, such as advertising or commerce policies. If it does, Facebook removes the content. If it doesn't violate our Community Standards, then Facebook will further assess if the content violates the law in that country, and if it does we generally block access to it in that country.

When a photo, video or post has been removed under the Community Standards, in most cases the user who posted it is notified and is given the option to request a review. This leads to a review, typically within 24 hours. If on review Facebook has concluded the content should be restored, the user gets notified and the original posting is restored. For certain high severity content violations, Facebook may not allow users to request another review.

[3] For further details please see our response to Section A question 2

In order to give our community visibility into how we enforce policies, respond to data requests and protect intellectual property, while monitoring dynamics that limit access to Facebook products, we publish regular transparency reports and other information:

- a dedicated IP Transparency Report and detailed IP Help Center;
- a report on Content Restrictions Based on Local Law, detailing instances where Facebook has limited access to content based on local law;

As noted above, because of the way content is assessed, if it had previously been determined to violate Community Standards, it may not appear in the illegal content transparency report. Facebook also regularly publishes a report including metrics on violations of many of our Community Standards, which - as previously mentioned, may include content that would also be considered unlawful in some jurisdictions.

The regulations could incentivize public reporting on community standards and could possibly include measures such as how much content was removed, under what category, and how it was identified (proactively or through users' reports) and the prevalence of such content (i.e. how often such content appears on the platform).

Regulation should clarify and substantiate the questions that are important for platforms to answer through such reporting and platforms should be able to independently assess what measures correctly answer those questions.

In order to be truly meaningful, the reporting of specific metrics should be done in the framework of helping policy-makers properly understand the state of the platforms and their efforts. Where needed such understanding should be aided by accurate narratives on how the platforms are evolving.

Measuring the right metrics that actually help answer the right questions is not a trivial endeavour and requires a massive understanding, detailed caveats and significant effort in terms of human resources, processing time and financial commitments. In a number of cases, measurement such as retrospective analysis may not always be feasible. Hence, systematic transparency should always be preferred over ad-hoc requests for metrics.

There is an opportunity to work with policymakers to co-develop agreed-upon questions that platforms should answer and develop metrics that can be systematically and accurately measured and reported over long periods of time to answer said questions.

18 **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

Facebook publicly shares information on a regular basis through the Community Standards Enforcement Report, that includes information about content that is removed from the platform because it violates our Community Standards. This Community Standards Enforcement Report also includes information regarding content detected and removed with the help of AI tools. We also regularly share other transparency reports regarding take-down requests for illegal content in specific countries, as well as Intellectual Property violations.

Whilst Facebook understands the desire for a broader range of competent authorities, social researchers and other civil society to have access to more information, there are a number of potential concerns. Therefore, it would be desirable to have this coordinated through a voluntary cooperation scheme. In particular, there are concerns relating to too much specifics when sharing details of how algorithms operate which could enable bad actors to more effectively circumvent detection mechanisms.

Not all platforms are the same, and therefore will not be able to have the same type of systems in place nor information available. We believe it is essential to have a structure of protection regarding any information shared with authorities. Care needs to be taken regarding:

- *information requests to ensure those serve specific and defined regulatory functions.* In particular with AI-related information there is a process of continual development and improvement, and information in relation to this, should be within that context and understanding.
- *designating who is or isn't a trusted researcher, and for what purpose they want information*. There are risks associated with information becoming available that would allow bad actors to 'game' the platform and exploit systems.
- *Ensuring respect for user privacy and data*, as well as for company confidential information.
- *the legal basis for the information sharing* – if the information includes personal data then the information sharing must be compatible with the GDPR; if the information contains proprietary or confidential material, appropriate measures must be put in place to safeguard those rights.
- *what is necessary and proportionate to the objective* – the information must service specific and defined objectives, underpinned by the need for good regulatory

outcomes. Furthermore, the information shared must be proportionate to that objective.

- *what is technically feasible* – not all platforms are the same, and therefore will not be able to have the same type of systems in place nor information available. In addition, the utility of information will change over time, for example with AI-related information there is a process of continual development and improvement, and information in relation to this, should be within that context and understanding.
- *security* – careful consideration needs to be given to the security implications of sharing the data with third parties – be that the information security risks posed by providing access to a dataset by a third party; and/or the risk of bad actors gaming the platforms and exploit systems once information becomes more widely available.

There is no single "one size fits all" answer here; much depends on the facts in hand, case by case, for each information sharing request. Given that the service provider is uniquely placed to assess each of these issues, in our view it would be desirable to have this coordinated through a voluntary cooperation scheme.

It is worth noting there is no universal concept of an illegal user account, although Facebook does a lot of work to remove inauthentic accounts and publishes details of this work regularly. We block millions of fake accounts every day when they are created and before they can do any harm. This is incredibly important in fighting harmful content such as spam, fake news, misinformation and non-compliant ads. Our machine learning takes a sophisticated and holistic approach to analysing user behaviour that takes in around 20,000 features per profile; for instance, it'll take into account the friending activity of an account the suspicious and potentially fake account sent a friend request to, and not just the suspicious account itself. The goal is to combat the ways malicious actors replicate genuine behaviour.

19 **In your view, what measures are necessary with regard to algorithmic recommender systems used by online platforms?**
5000 character(s) maximum

Facebook is aware that there can be many interpretations of what is meant by an algorithmic recommender system, and in response to this question we are using the definition provided by Profs. Francesco Ricci, Lior Rokach, and Bracha Shapira, authors of the 'Recommender Systems Handbook.' *"Recommender Systems (RSs) are software tools and techniques providing suggestions for items to be of use to a user. The suggestions relate to various decision-making processes, such as what items to buy, what music to listen to, or what online*

news to read."[4] This is distinct and different from content that the user chooses to follow. Noting that these systems are automated in nature, designed to both enhance and protect the user experience.

When users have a greater understanding of the factors that might be used to recommend the content that is served to them, they are better able to recognise where the content is from. This awareness leads users to appreciate how recommender systems can work and improve understanding of the product as a whole

There is a lot of policy debate around algorithmic transparency, but the regulatory response 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. That said, Facebook does consider it important that users know the principles behind our recommendation systems.

We make automated personalized recommendations to the people who use our services to help them discover new communities and content. Both Facebook may recommend content, accounts, and entities (such as Pages, Groups, or Events) that users do not already follow. Some examples of our recommendation experiences include Pages You May Like, "Suggested For You" posts in News Feed, People You May Know, or Groups You Should Join.

Our goal is to make recommendations that are relevant and valuable to each person who sees them. We work towards our goal by personalizing recommendations, which are unique for each person. For example, if you and another person have Facebook Friends in common, we may suggest that person as a potential new Friend for you.

We take steps to avoid making recommendations that could be low-quality, objectionable, or insensitive. While we remove content that violates the Community Standards, we take additional steps when it comes to recommendations in order to provide a quality experience for users and avoid recommending certain content even if it does not violate our Community Standards.

Not all platforms are the same, so determining what information should be made available or what measures in relation to algorithmic recommender systems, may not be a 'one size fits all' solution. For Facebook, principles should include transparent information about the

[4] Ricci, Francesco, Lior Rokach, and Bracha Shapira. "Introduction to recommender systems handbook." Recommender systems handbook. Springer, Boston, MA, 2011. 1-35.

factors that influence how algorithmic recommendations are made, and when major changes are made, how these affect the user.

Additionally, care needs to be made to not be overly prescriptive, changes are made regularly based on user feedback, so any requirements need to ensure that companies can innovate without restrictive measures.

20 **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 tax collection, for the purpose of collecting 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
- ❑ **X Specific request of law enforcement authority or the judiciary**
- ❑ **X On a voluntary and/or contractual basis in the public interest or for other purposes**

21 **Please explain. What would be the benefits? What would be concerns for the companies, consumers or other third parties?**
5000 character(s) maximum

The private and public sectors should be encouraged to assess data sharing opportunities and determine, on a case-by-case basis, through voluntary contractual arrangements, how they can best achieve the full potential of data partnerships. We believe that greater collaboration can play a role in helping to address the challenges facing society today. The COVID-19 pandemic has shown that a role can be played by certain entities to work together with authorities to contribute aggregated data to benefit the public interest. This should not be limited to health-related research, but also for aspects relating to municipal or regional challenges such as improving mobility, addressing environmental challenges, and for supporting humanitarian crisis response. When personal data is involved, we support the idea of making it easier for those individuals that want to share data to do so.

22 **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

Should the regulation foresee a regulator to oversee rights and obligations of platforms, the regulator should not be empowered to review decisions made by intermediaries in relation to individual pieces of content, and regulatory sanctions would be appropriate only in the case of systemic failure. As the purpose of regulation is to bring good outcomes, it is typically not helpful to set up regulatory bodies that exclusively have fining power (without the option to issue guidance - binding or non-binding or offer the ability to remedy - instead of fines, or as a first step). Such failure would be assessed through a legal and principle based approach set by the legislator. Safeguards would need to be included for all parties. The regulatory model would then be driven by a focus on best practice - not simply compliance. Therefore, incentives for investment in best practice systems should be a key feature.

Facebook considers any regulatory measures should be applied proportionality, and this should be assessed according to the characteristics and nature of the service and the risk that is posed. The wrong incentives could discourage growth and diversification, particularly if growth would mean additional regulatory burdens.

23 **Are there other points you would like to raise?**
3000 character(s) maximum

n/a

LIABILITY REGIME

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)**

5 stars (very important)

The harmonised liability exemption regime has been essential to the development of an innovative, successful online environment and a vibrant online economy in the EU. It is one of the key mechanisms balancing freedom of expression and information with other fundamental rights. Facebook strongly supports the preservation of the essential features of this regime in the DSA and makes constructive suggestions below as to how the regime can be clarified and improved.

2 **The liability regime for online intermediaries is primarily established in the ECommerce Directive, which distinguishes between different types of services: so called 'mere conduits', 'caching services', and 'hosting services'. In your understanding, are these categories sufficiently clear and complete for characterising and regulating today's digital intermediary services? Please explain.**
5000 character(s) maximum

The internet landscape has certainly changed since the adoption of the E-Commerce Directive, but Facebook believes that the category of "hosting services" (which is the category of relevance to Facebook) remains sufficiently clear (as interpreted by relevant jurisprudence across the Member States) for characterising and regulating today's digital intermediary services.

Case law, including in the CJEU, has consistently recognised that the current definition of a "hosting service" in Article 14(1) of the E-Commerce Directive ("*an information society service … that consists of the storage of information provided by a recipient of the service*") squarely encompasses the Facebook service. *See, e.g.*, *Glawischnig-Piesczek v Facebook Ireland Ltd* (Case C-18/18, Judgment of 3 October 2020).

However to avoid ambiguity and to empower hosting services to act as a "diligent economic operator" (as per *L'Oréal v eBay* (Case C-324/09), and supported further by the objectives of the European Commission in its 2017 and 2018 Recommendations, Facebook advocates for the removal of and/or clear amendment to, the limitation contained in recital 42 to the Directive that appears to restrict the exemptions from liability to activities which are "*of a mere technical, automatic and passive nature, which implies that the information society*

service provider has neither knowledge of nor control over the information which is transmitted or stored." (emphasis added). As explained further below in the responses to questions 4 and 5, this limitation is incompatible with the robust internet that has developed since the promulgation of the E-Commerce Directive, and could be interpreted so narrowly as to apply only to those intermediaries that have no engagement whatsoever with users' content, such as pure bulletin-board services. Simply because the internet experience in 2000 was not as rich as it is now does not mean that today's intermediaries should be excluded from the safe harbour or uncertain of their ability to avail of it. Indeed, the E-Commerce Directive was intended to incentivize innovation and the growth of the internet. But such a strict interpretation of recital 42 could foreseeably prevent or discourage online intermediaries from exploring innovative and personalised user experiences and from taking voluntary proactive steps to identify and remove unlawful or harmful content. Indeed, Advocate General Saugmandsgaard Øe acknowledged as much when he noted in his recent opinion in *Peterson v. Google LLC* that neither automated recommendations nor proactive checks of content should be sufficient to indicate that an intermediary plays an "active role" under the E-Commerce Directive.

Although the three categories of mere conduits, caching services and hosting services referred to in Articles 12, 13 and 14 of the Directive valuably cover many online intermediary services, Facebook is aware that there remains uncertainty as to whether these categories embrace other kinds of service. Given the rapid technological development of an increasingly diverse range of online intermediary services, and the inclusion of a search component in many hosting services, Facebook suggests adding a fourth category of online intermediary service which qualifies for the limited liability regime, which could expressly include, for example, search engine services, providers of hyperlinks and content aggregators, and also extend to other online intermediary services of a similar nature to mere conduits, caching services, hosting services or search engine services to provide some degree of flexibility and to future-proof the legislative framework. This was raised by Advocate General Jaaskinen in his opinion in the *Google Spain* case (Case C-131-12, Opinion of 25 June 2013) at para 38 ("*it is necessary to analyse their position vis-à-vis the legal principles underpinning the limitations on the liability of Internet service providers. In other words, to what extent are activities performed by an Internet search engine service provider, from the point of view of liability principles, analogous to the services enumerated in the Ecommerce Directive*").

Overall Facebook strongly supports preserving the horizontal liability regime which applies to these categories of online intermediaries, and which over the years has allowed the emergence of countless types of new digital services and the development of a thriving online ecosystem. Facebook welcomes the opportunity to work with the European Commission to ensure that the limited liability regime works for the modern digital environment and provides as much clarity and certainty as possible to a broad range of online intermediary

services, whilst enabling and encouraging such services to take necessary voluntary proactive steps to ensure the safety of its online community.

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 elements that require further legal clarification?**
5000 character(s) maximum

Facebook believes the knowledge standard applicable to hosting services has been essential to the development of an innovative internet economy in Europe and the protection of fundamental freedoms such as freedom of expression and user privacy. The rule that hosting services cannot be held liable for their users' wrongdoings as long as they act expeditiously once they have actual knowledge of specific clear illegality, while not without its own challenges, has achieved a balance between protecting those rights whilst allowing timely, proportionate actions against clearly illegal content and activities.

Nevertheless, there is room for clarification in three areas.

(1) A single standard of actual knowledge of illegality should apply to both caching and hosting services. Currently, Articles 13 and 14 of the Directive appear to set different standards for caching services versus hosting services, with the former subject to a clear standard of actual knowledge while the latter are required to act upon actual knowledge *or* awareness. It is not clear why these two different formulations of the knowledge standard are used. In Facebook's experience the inclusion of the formulation "aware of facts or circumstances from which the illegal activity or information is apparent" leads to arguments about what the provider *should have known* (constructive knowledge) rather than what it *did know* (actual knowledge). The standard of awareness of facts or circumstances from which the illegal activity or information is apparent is unnecessary, confusing and should be deleted. Actual knowledge of illegality should be the standard for both caching and hosting services. The legislation also should confirm that by being placed on notice of specific illegal content, the intermediary's obligations and consequent eligibility for the safe harbour apply only to that particular content and are not subject to review or scrutiny platform-wide.

(2) The question of whether intermediaries have actual knowledge of illegality should be based on a "reasonable layperson" standard, meaning that the illegality must be clearly apparent on its face to a person without specialized expertise or contextual knowledge. This standard, which already exists in some Member States, recognises that it is simply unreasonable to expect intermediaries and their employees to be versed in every law of every Member State and be able to determine whether any given piece of content violates any of those laws and instead focuses on whether content is obviously illegal. The reasonable layperson standard also accounts for the fact that, in many circumstances, identifying illegal activity or information requires additional context, which an intermediary simply may not have. If intermediaries are held to a different standard than the reasonable layperson, there is a real risk that they will be incentivised to over-block content in an attempt to bridge this knowledge gap and avoid liability. This will lead to a chilling effect on freedom of expression and information. The reasonable layperson standard appropriately balances incentives by ensuring that intermediaries are not found to have actual knowledge of content that may not be obviously illegal (e.g., intellectual property infringement, defamation, or low-level invasions of privacy) while also encouraging intermediaries to remove obviously illegal content, which is the content that is most likely to cause harm (e.g., child exploitation imagery).

(3) The legislation should clarify the minimum information to be included in a removal request to intermediaries. Facebook has strong policies, systems and procedures in place to promptly address such notifications (see response to Part A of the first module above). However, these can only work effectively if the notification (a) clearly identifies the content in question to enable the intermediary to locate the content quickly and easily, and (b) contains a clear explanation of why it is illegal. Setting out the minimum information required for a valid notification would provide more certainty and clarity for all intermediaries and may be particularly helpful for smaller intermediaries with more limited resources, which will lead to more efficient processing of notifications across the ecosystem. These minimum requirements should include the name and contact information of the reporting party, the URL (assuming it is available), the local law the content is said to violate, a brief explanation of why the content violates that provision or legal rule, supporting evidence to demonstrate why the reporter believes the content is clearly unlawful where appropriate (e.g., evidence of a rights holder's registered trademarks for a counterfeit report), and the relevant court order, if available. Notifications that do not meet these minimum requirements should not impute actual knowledge to intermediaries. Nor should intermediaries be considered to have actual knowledge of illegality beyond the legal provisions identified in the report.

The notification should also include the standing or position of the notifier so that the intermediary can assess whether the notification is made in good faith. Facebook has had experience of notifications which are abusive or made in bad faith (e.g., by submitting fraudulent or over-reaching reports seeking to use intellectual property as the basis to remove legitimate speech). Abusive or bad faith notifications should be subject to penalties and/or liability, and intermediaries should be permitted to ignore notifications which they have reasonable grounds for suspecting are made in bad faith.

4 **Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected.**
5000 character(s) maximum

It is in service providers' interest - and the interest of their users and the community at large - to take responsibility to proactively reduce the appearance of unlawful or harmful content on their platforms, even if not legally required to do so. And yet doing so can expose service providers to the risk of losing the very protection that enabled the internet to grow and thrive in the first instance. Specifically, the current legislative framework disincentivises platforms from undertaking voluntary proactive measures against illegal or harmful content, because as currently framed, it risks any platform that undertakes such measures (which may necessitate manual review in addition to pure automation depending upon the circumstances) being framed as more than a merely "technical, automatic and passive" intermediary and thus arguably excluded from the Directive's safe harbour. Indeed, the current regime introduces the perverse result that by undertaking more than is legally required to reduce the prevalence of unlawful or harmful content on their platforms, intermediaries may be found to exercise too much control over content, or to have somehow acquired knowledge of unlawful content, such that they could be held liable if their enforcement in that regard proves imperfect. Advocate General Øe acknowledged as much in his recent opinion in *Peterson v. Google LLC* when he noted: "*it is necessary to avoid an interpretation of the concept of 'active role' that could produce the paradoxical result whereby a service provider conducting research on its own initiative into the information which it stores … would lose the benefit of the exemption from liability laid down in Article 14(1) of that directive and would, therefore be treated more severely than a provider which does not.*" Without any provision under the law to protect intermediaries from this result, they are naturally disincentivised from doing any more than the minimum legally required, to avoid otherwise being considered to be active intermediaries or to have actual knowledge of clearly unlawful content under their control.

Facebook would therefore welcome the introduction of a provision under the legislative regime that would incentivize intermediaries to undertake proactive measures to tackle harmful or unlawful content. Such a provision should provide broad protections that make clear that undertaking such efforts does not risk the intermediary being precluded from the definition of a "hosting service", nor should it be deemed to have actual knowledge of unlawful content merely by reason of undertaking such measures.

In its 2017 Communication on Tackling Illegal Content Online, the Commission helpfully sought to reassure intermediaries that undertaking proactive measures to reduce the prevalence of policy-violating or otherwise unlawful content should not affect their ability to rely on the safe harbour provisions of the E-Commerce Directive. However, as stated, the protection seemed to apply only insofar as the initial decision to undertake proactive measures; by its definition, the taking of such proactive measures may impute onto the intermediary actual knowledge or awareness of arguably unlawful content under Article 14, such that unless it expeditiously removed or disabled the content in question, it would lose safe harbour protection. Understood in this way, this would be hardly any protection at all, as it would require the intermediary to expeditiously remove any content its proactive measures might identify, and any potentially unlawful content that is not captured (as is likely with imperfect technology, adversarial bad actors and the importance of context in determining illegality in many instances) would give rise to liability.

To properly address this counter-intuitive result, Facebook strongly supports the introduction of a provision that makes clear that the taking of proactive measures, including the use of algorithms, machine learning, or other technological measures, to detect, remove or disable access to unlawful or otherwise harmful content shall not amount to knowledge or awareness for purposes of Article 14(1)(a), nor shall it be deemed to make the intermediary an "active" one for purposes of eligibility for the E-Commerce Directive's safe harbour.

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 explained in the response to questions 2 & 4 above, the limitation in recital (42) to the Directive, which appears to restrict the availability of the exemptions from legal liability to service providers whose activities are of *"a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored*", is a feature of the current

regime that risks disincentivising hosting service providers from taking proactive measures against illegal or harmful content.

Facebook has concerns that restricting the exemptions to unclear concepts of active versus passive and requiring only technical or automated activities is no longer fit for purpose. Moreover, this distinction is entirely counter-intuitive to a service providers' ability to keep its platform safe, whilst not resorting to only blunt technical solutions. Such automated solutions would inevitably lead to over-blocking and have a material and significant impact upon free expression and the societal value of online communities and expression generally.

There is widespread impetus globally for online intermediaries to act diligently and responsibly in respect of illegal and harmful content, and a number of service providers (like Facebook) currently engage in a large number of automated and manual voluntary measures to better enforce their terms of service and policies and to protect their users and community. As noted in response to Question 4 above, intermediaries should be actively encouraged to take active voluntary measures in this way, without introducing uncertainty as to whether such activities either (1) take them outside of the safe harbour or (2) impute the intermediary with knowledge of unlawful content. The legislation should also enshrine the principles from CJEU case law that the use of technical and automated means, such as artificial intelligence or machine learning classifiers, do not impute actual knowledge or awareness of illegal content on service providers.

The current lack of clarity in this regard is demonstrated by the request for a preliminary ruling in *Puls 4 TV GmbH & Co. KG v YouTube LLC and Google Austria GmbH* (Case C-500/19) seeking guidance from the CJEU as to whether steps taken by YouTube (such as sorting, tagging and recommending content to users, and providing assistance in uploading content) amount to an "active" role. It is also demonstrated by the difficulty in reconciling the European Commission's view about the width of this concept in its "Tackling Illegal Content Online" Communication with some of the relevant case-law of the CJEU. The Commission makes clear that online platforms can and should take proactive measures to, for example, detect and remove illegal content online (particularly where those measures are taken under the platform's terms of service) without losing the protections of the safe harbours; indeed, as AG Saugmandsgaard Øe observed in the YouTube Opinion, "a provider cannot be considered to play an 'active role' with regard to the information it stores merely because it proactively carries out certain checks . . . to detect the presence of illegal information on its servers" as "is clear from recital 40 of Directive 2000/31." Nevertheless, the relevant case law from the CJEU (such as *L'Oreal v eBay*) appears to be more qualified and circumspect in its determination as to what activities or "steps" can be undertaken by an online platform without falling foul of the principles of recital 42 (e.g., limited to storing offers for sale on the

provider's server, setting the terms of its service, receiving remuneration for that service and providing general information to its customers).

In order to reconcile these historic positions and provide greater clarity to online intermediaries and to incentivise voluntary and proactive enforcement measures, Facebook strongly supports the removal of recital 42 and / or an amendment which ensures that in addition to data storage, standard industry-wide commercial activities of online intermediaries deployed to operate and host a platform and optimise the user experience (including but not limited to sorting, tagging, providing "Help" resources, recommending content to users), as well as taking proactive steps to detect, remove or disable access to illegal or harmful content to keep online communities safe are acknowledged as activities that can be undertaken within the parameters of Article 14 and its safe harbour.

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

Facebook regards as vitally important the prohibition in Article 15 of the Directive of the imposition by Member States of general monitoring obligations or obligations actively to seek facts or circumstances indicating illegal activity. This prohibition not only remains appropriate but is central to the proper functioning of the intermediary liability regime and to the appropriate safeguarding of freedom of expression and other fundamental rights. Moreover, if such general monitoring obligations could be imposed on service providers, it could defeat or seriously undermine the safe harbours conferred by Articles 12-14, which are conditional on the service provider not having actual knowledge or awareness of illegal activity.

There are, however, provisions relating to proactive monitoring that could bear some clarification. In particular, while the Directive provides, and the CJEU has consistently held, that an intermediary cannot be compelled to undertake an obligation to actively monitor all the data of all its customers, there remains a lack of clarity as to recital 47's allowance of "monitoring obligations in a specific case."

In practice, depending on the way in which an order is framed, monitoring obligations in a specific case can have the practical effect of requiring the general monitoring of all the intermediary's data of all its customers, which would clearly run afoul of Article 15's prohibitions. An example of this result can be seen in *Glawischnig-Piesczek v Facebook Ireland Ltd*, where the CJEU decision held that a court from a Member State is not precluded by Article 15 from ordering the removal of identical or "*equivalent*" content to that which had been declared illegal. What the precise denominations of "identical" and "equivalent" mean in practice remains unclear and the decision (which is yet to be interpreted by the national referring court) gives little to no regard to technical feasibility or the practical effect on potentially legitimate speech. The CJEU decision in *Glawischnig-Piesczek* attempts to provide some clarity by limiting "equivalent content" to that which is "essentially unchanged", such that the online platform may rely on automation and need not carry out a separate assessment of unlawfulness. However, uncertainty as to how this might be interpreted remains and without clear legislative guardrails, national courts will continue to impose expansive and prohibited general monitoring obligations upon online intermediaries. In doing so, they will continue to implement their own inconsistent standards of equivalence, which in reality will necessitate general monitoring and human review and judgement.

These concepts could be clarified in legislation, for example by explicitly providing that monitoring "in a specific case" should apply only to proportionate measures relating to the identical content posted by the same user or at most should be limited to the service provider's technical capability (on a case by case basis) to monitor and enforce against identical or, from a technical perspective, near identical content (i.e., near exact duplicates) of the illegal content. Any obligation that stretches beyond that scope would necessarily involve the evaluation of the content posted by all users, as well as the context and circumstances in which it is posted, which would virtually by definition constitute a "general" monitoring obligation. Such a formulation also would "avert the risk of intermediary providers becoming judges of online legality" at "the risk of 'over-removal,'" as Advocate General Øe recently noted.

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

Facebook supports the introduction of a harmonised EU framework for content regulation, and we support regulation of both illegal *and harmful* content in the EU. The regulation of content that is harmful but not illegal should be in parallel to the regime that governs limited legal liability for illegal content. This topic is addressed in detail in Facebook's responses to the relevant questions in the previous module. Our experience is that there is little

coordination within the single market, which creates market fragmentation. There are already issues of having to manage enquiries and requirements from multiple regulators without formal jurisdiction, that imposes not only a heavy burden (for example with take down notices or litigation), but also creates the risk of having competing requirements in neighbouring countries which should be avoided.

In essence, Facebook believes that intermediaries should be responsible for putting systems in place for the removal of specific categories of harmful but lawful content. Driving up standards of the systems employed by the operators is likely to result in greater progress than penalising them for individual failures to remove reported content that is harmful but not illegal.

By way of example, to support platforms in developing their own bespoke systems, a regulator could require intermediaries to consult with external experts and stakeholders to develop content policies as appropriate and which address content which is perceived to be harmful although not unlawful, put in place or improve systems for processing reported content in order to enforce such policies, provide an appropriate system of internal or external appeal against enforcement decisions, and report publicly on the effectiveness of their systems in reducing the types of content targeted. Any regulator would not review decisions made by intermediaries in relation to individual pieces of content, and regulatory sanctions would be appropriate only in the case of systemic failure.

Any regulation should recognise the need to balance the removal of harmful content with the protection of freedom of expression and other fundamental rights. Holding intermediaries liable if they do not remove individual pieces of third-party content will necessarily lead to overblocking of content, as intermediaries will be wary of incurring penalties and/or fines. Regulation should also recognise that intermediaries face challenges when they *do* seek to remove harmful content pursuant to their policies. At an increasing rate Courts in a number of Member States are regularly ordering Facebook to reinstate content that violates Facebook's Community Standards -- and would be considered by many to constitute harmful content. These "wrongful removal and restoration" decisions limit Facebook's ability to remove harmful content and keep its platforms safe, and regulations should acknowledge that intermediaries cannot be held liable if they in good faith remove content from their platform in an effort to combat harmful speech.

EX ANTE MEASURES

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

	1 (fully agree)	**2 (somewhat agree)**	**3 (neutral)**	**4 (somewhat disagree)**	**5 (fully disagree)**	**I don't know / No answer**
Consumers have sufficient choices and alternatives to the offerings of online platforms.	x					
It is easy for consumers to switch between services provided by online platform companies and use same or similar services provider by	X					

other online platform companies (“multi-home”).						
It is easy for individuals to port their data in an useful form for alternative service providers outside of an online platform.		X				
There is sufficient level of interoperability between services of different online platform companies.				X		
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						X

conditions.						
It is easy for innovative SME online platforms to expand or enter the market.	X					
Traditional businesses are increasingly dependent on a limited number of very large online platforms.					X	
There are imbalances in the bargaining power between these online platforms and their business users.				X		
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.					X	

Certain large online platform companies create barriers 30 to entry and expansion in the Single Market (gatekeepers).				X		
Large online platforms often leverage their assets from their primary activities (customer base, data, technological solutions, skills, financial capital) to expand into other activities.				X		
When large online platform companies expand into such new activities, this often poses a risk of reducing innovation and deterring competition from					X	

smaller innovative market operators.						

Main features of gatekeeper online platform companies and main relevant 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	**OX** OOOO
Wide geographic coverage in the EU	**OX** OOOO
They capture a large share of total revenue of the market you are active/of a sector	**OOOX** OO
Impact on a certain sector	**OOOX** OO
They build on and exploit strong network effects	**OOX** OOO
They leverage their assets for entering new areas of activity	**OX** OOOO
They raise barriers to entry for competitors	**OOOOOX**
They accumulate valuable and diverse data and information	**OOX** OOO
There are very few, if any, alternative services available on the market	**OOOOX** O
Lock-in of users/consumers	**OOOOX** O

Other	OOOOO

2 If you replied "other", please list
3000 character(s) maximum

N/A

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

There is an intrinsic difficulty in relying on this type of patchwork definitional process for what does or not determine a 'gatekeeper'. The Commission seems to be suggesting a sweeping definition that would not require any process to define a market and capture entire corporate groups. Without the ability to determine what market is being considered for regulatory intervention - much of the categorisations will struggle to effectively assess market failure and as a consequence will likely be unable to accurately determine any success of market intervention or any relevant measure of proportionality. If a regulatory proposal only defines the type of company it aims to regulate and doesn't determine the market - the remedy risks being inappropriate and harming consumer welfare by stifling innovation. We would suggest that the Commission follow other precedents of ex-ante regulatory intervention and build a robust, transparent and comparable model for market assessment for the sake of all parties. Facebook also notes that the use of generic criteria to define the notion of 'gatekeeper" would not be appropriate. A large user base, for example, is not particularly relevant unless users are locked in. Likewise, the ability to enter into new markets by using existing assets and advantages can hardly be a distinguishing factor as that is a common theme across industry and is pro-competitive and consumer welfare enhancing. This suggests, at a minimum, that assessing 'gatekeeping companies' on a case-by-case basis certainly is more sensible than determining scope on the basis of broad and vague criteria.

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 strengthen 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
- ❑ **X 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
- ❑ **X other. Please specify in the text box below.**

5 **Other - please list**

Integration of new features generally gives rise to clear consumer welfare effects. Indeed, the integration of new services may be efficient or irrelevant for a user of another service on a platform depending on the nature, quality, and form of the integration. Similarly, it may or may not have an impact on switching or multi-homing opportunities. The impact, rather than the type of service per se, is what needs to be evaluated. It is also important, through a process of market definition and assessment, to determine whether features that arise within a market are transitory or persistent and as a result whether the combination of certain business operations leads to a stronger operational organisation or simply a number of business lines that have little impact on each other. While there may be certain parts of any individual company's operation which may raise questions, those questions will not generally extend to the entire company or corporate group.

Emerging issues

.

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

- ❑ **X 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

Facebook is a developer that uses the app stores on both major mobile smartphone operating systems to distribute its apps. We have encountered challenges related to app distribution and monetization on Apple's mobile operating system, iOS, and its associated App Store. Apple's iOS is one of two mobile smartphone operating systems on consumer devices, and the only one available on Apple devices. The App Store is effectively the only way for developers to reach consumers on Apple devices. Like any app developer, we have faced challenges in the application of Apple's policies and technical controls around in-app payments, gaming apps, log-in tools, and online advertising. In each category, Apple has made policy and enforcement decisions that privilege its own services and revenue streams to the detriment of others. We describe these policies and practices and their impacts on our business, consumers, and other stakeholders in more detail below.

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

Yes, we have been affected by unfair contractual terms and unfair practices imposed by Apple with respect to the App Store and on iOS more broadly. The Facebook Gaming app is a focused, gaming-only experience where people can watch streams of others playing games, play instant games, and take part in gaming groups. We launched the Facebook Gaming app in Google's Play Store for Android in April 2020 and Apple's iOS App Store in August. The delay in launching the iOS version of Facebook Gaming is attributable to several rejections of the app submitted to Apple's App Review, for alleged violations of App Store Review Guideline 4.7, which prohibits apps with the "main purpose" of distributing casual games. The version of the Facebook Gaming app that ultimately launched for iOS in August 2020 does not include playable games. The iOS version of Facebook Gaming does not include playable games, unlike the Android version. Thus, consumers on iOS have a sub-optimal experience compared to those using Android. Overall, fewer Facebook users will be able to engage with instant games in mobile settings. For Facebook, over the course of six months, we invested engineering time and resources in developing and submitting alternative versions of the iOS Facebook Gaming app in attempts to satisfy Apple's requirements while still enabling consumers on iOS to enjoy some aspects of the app. Apple rejected all versions that did not remove people's ability to play games from within the Facebook Gaming experience. This reduces the appeal of the app on iOS devices. Developers that take advantage of Facebook Gaming as a mobile gaming platform also lose significant opportunity to engage with and attract new users on iOS because people

cannot play their games. If App Store Review Guideline 4.7 is applied to the distribution of cloud games accessed through streaming platforms, it will reduce the incentive of developers to create new games that take advantage of the benefits of cloud gaming. With regards to Apple it is well known that mobile games are the most lucrative category of mobile apps worldwide. A significant portion of Apple's mobile OS revenue comes from purchases of games distributed directly through the App Store, and purchases made from within those games. By largely prohibiting other developers from offering apps that enable consumers to access games not directly distributed through the App Store, Apple is ensuring that consumers on iOS can primarily purchase games and related services only from Apple, and not from other developers.

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

Yes. We are particularly concerned about policy changes that may affect developers' ability to offer services that compete with the platform's own services. For example, large operating system/app store platforms increasingly are imposing tight restrictions around developers' access to data and to combine data collected across different apps and websites. These activities have long been important to advertising services' ability to deliver and measure relevant advertising, and their restriction threatens to harm ad-supported online services and the consumers that rely on them. Perhaps more concerning, it is unclear whether the large platforms imposing these restrictions will themselves be subject to such restrictions - or whether their own increasing advertising efforts will continue without such restraints either by not applying the same constraints on their own services or by leveraging solutions they don't make available to third parties (e.g. support for cross app understanding and background computing on-device). Moreover, we are concerned these restrictions may also be motivated, in part, by the platforms' own business interests such as the increased revenue that some may attain by pushing developers toward in-app payments, of which platforms often claim a significant portion.

7 **Have you considered any of the practices by large online platform companies as unfair? Please explain**.
3000 character(s) maximum

Please see the other answers to this section.

The following questions are open to all respondents.

9 **Are there specific issues and unfair practices you perceive on large online platform companies?**
5000 character(s) maximum

We believe that terms and conditions and the processes around how all users of platforms stay informed should be clear and transparent - ensuring that users have adequate notice to any changes in their service is important. Decisions should not be arbitrary and should there be further dispute, an adequate dispute resolution mechanism may be appropriate to ensure that all parties have a fair and transparent process that allows for a timely resolution to any discrepancies. Any intervention should empower users and businesses to evaluate performance and commercial opportunities.

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

We view relatively few challenges in regard to the use and sharing of data other than the development of business and commercial relationships in the data ecosystem. The nature of data which is non-rivalrous, reusable and easily accessible - for user-directed sharing of personal data Facebook offers data portability tools like Download Your Information and participates in the Data Transfer Project, a collaboration of organisations, including Apple, Google, Microsoft and Twitter, committed to building common ways for people to transfer data into and out of online services whilst balancing privacy and security. Even more firms are offering similar portability services as a result of measures like the General Data Protection Regulation and many other initiatives. Data portability can assist people with the process of joining or trying a new app or service by enabling them to easily transfer profile information and data that would be relevant or useful to them in the new context. It should be noted that for online services that are part of, or bundled with, embedded operating systems (e.g. most mobile phones and personal computers), portability alone may not be as impactful as it can be

for online services that are device independent. This is because having online services bundled with a device makes the cost of switching or multihoming higher, often including the price of a new device. Our Download Your Information tool allows users to request to download a single data file in HTML or JSON format, which can then be uploaded to a new provider. Our new data portability tool based on the Data Transfer Project enables users to transfer all of their photos or videos to a new provider in a one-off transfer. The transfer can be repeated at the user's initiation. We have previously written about the data protection challenges of data portability and we believe that organizations should give people control over their information by enabling them to take it out of one service and bring it to another. But even in jurisdictions with laws already in place—and certainly where they are being considered—we think there are fundamental questions that need to be answered for portability to be implemented successfully—meaning we can build privacy-protective, easy-to-use products for users. Amongst others, these questions include What is data portability? Is every user-directed transfer a "data portability" transfer? What kind of data should be portable? Should it just be information I share on a service? Information about my use of the service? Whose data should be portable? Should I be able to take my friends' data to another service? How should we protect privacy while enabling portability? Should we evaluate the places people want to port their data? Should we refuse to fulfill requests if we think recipients could be bad actors? And how should we enable people (and their friends) to make informed choices about porting data? After people's data is transferred, who is responsible if the data is misused or otherwise improperly protected? Is it solely the responsibility of the recipient, or does the transferring company (or requesting person) bear that responsibility? Facebook works with the wider industry to explore and expand upon similar questions about trustworthy data sharing from a cross-sectoral point-of-view. We're also participating in innovative projects such as the Data Mobility Sandbox from June 2019, which explored the conditions for the safe porting of personal data through data facilitator models, a multilateral model for user-directed sharing of data through portability requests. The next stage of this collaborative research project in 2020 explores how cross-sectoral value can be generated through data mobility, mitigating risks and obstacles while accelerating potential service opportunities. The current phase of this project involves rapid co-creation and testing of diverse service experiences to assess the desirability of future-facing portability scenarios. As a general comment, any data sharing mechanisms will need to take account of three key considerations: 1) the protection of users' personal data; 2) the protection of business users' sensitive commercial data; and 3) the legitimate protection of a company's IP and trade secrets.

In the context of the DSA, we would like to encourage the Commission to keep in mind what objectives they are trying to achieve through regulation and how those regulations will shape products and user behaviour in practice, also in light of data portability. How people behave online heavily impacts our product decisions and should similarly inform regulatory and policy thinking. For example, people often multihome in their use of online services because of the

simplicity of browsing to another site or downloading another app. Portability can further support that kind of consumer behaviour. Data portability can assist people with the process of joining or trying a new app or service by enabling them to easily transfer profile information and data that would be relevant or useful to them in the new context. It should be noted that for online services that are part of, or bundled with, embedded operating systems (e.g. most mobile phones and personal computers), portability alone may not be as impactful as it can be for online services that are device independent. This is because having online services bundled with a device makes the cost of switching or multihoming higher, often including the price of a new device. As the Commission will propose new and revised rules to deepen the internal market for digital services, we encourage the Commission to consider the circumstances in which it would be most helpful to people to switch services and rely on data portability. For Facebook, the principle of data portability is meant to give people control and choice while also fostering innovation. That informs how we design our products and is consistent with our view on how regulation should approach data portability obligations.

11 **What impact would the identified unfair practices can have on innovation, competition and consumer choice in the single market?**
3000 character(s) maximum

It is difficult to provide a definitive answer but given that consideration we would highlight the advantage of a case by case assessment to be able to effectively examine the market and determine the appropriate remedy. There is already a high degree of innovation when it comes to data sharing, Facebook has a number of different ways in which other organisations can reap the benefits of Facebook's data in a privacy preserving way. Crowdtangle is a public insights tool from Facebook that makes it easy to follow, analyse, and report on what's happening with public content on social media. Facebook Data for Good uses a variety of technical tools to help our partners access and use data for disaster response, health, connectivity, energy access, and economic growth. Facebook Connectivity Analytics is a suite of business tools that helps operators and device manufacturers prioritize their network and product investments to improve the online experience for their customers - Empowering network operators and device manufacturers to make better business decisions and prioritize network investments. Facebook developer tools offer developers a number of different resources, including open source AI development tools, tools to scale businesses across the Facebook family of apps and ensuring developers have access to the next generation of AR/VR technologies. Building on the provisions laid out in the GDPR we believe that establishing industry driven models for effective and user driven data sharing in a privacy perspective can be a spur to the single market and can foster innovation and growth in the single market. As referenced previously, it is fundamental that any decisions, be it around data or otherwise, are taken to support and progress the Single Market and further aim at harmonisation.

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

Facebook operates in an environment that is rapidly evolving, dynamic, and highly innovative, in which established digital platforms, new entrants, and increasingly traditional market players, compete vigorously. The ability to offer products and services that attract users is the key driver of competition. Competition on the user side is based on providing the most enjoyable, useful, and meaningful experience. This is often spurred by an innovative idea that is differentiated from existing offerings. There are no barriers to developing new ideas. This is borne out by the many examples of successful new entrants over the last few years that have been able to enter digital markets by developing an attractive offering to meet or create new user demand. TikTok is a good example in the social media space while online video conferencing service Zoom offers valuable lessons in how fast a company can expand even in markets with many established players. By way of example, the most recent Ofcom Online Nation report states that: "some of the fastest-growing services during the coronavirus crisis are not owned by Google, Apple, Facebook, Amazon and Microsoft [...]. TikTok [...] increased its reach among adults in the UK from 5.4 million to 12.9 million between January and April 2020, while Houseparty, owned by Epic Games, increased from 175,000 to 4 million. Zoom [...] reached 13 million adult internet users in April 2020, up from 659,000 in January 2020." (Ofcom Online Nation - 2020 Summary report). In other words, within the first four months of this year TikTok more than doubled its reach among adults in the UK, while the reach of Houseparty and Zoom increased almost 23- and 20-fold respectively. Our observation in this regard is that platforms such as Facebook have been supportive of start-ups and scale ups, enabling them to grow and compete more effectively with larger established market players. Facebook's advertising-supported services enable users to communicate, to connect and share with their friends, families and wider communities, and discover meaningful and relevant content free of charge. Facebook's business model allows businesses to effectively target its large number of users with relevant commercial offers in an increasing number of ways. Moreover, online platforms such as Facebook have helped to democratise advertising, creating effective advertising opportunities for many businesses for which traditional alternatives, such as TV advertising or newspapers, would be too expensive or inefficient. Advertisers of all kinds and sizes can advertise and benefit from the affordable, innovative and efficient advertising solutions that online platforms have driven and brought to the market. These have enabled advertisers (and particularly SMEs) to reach their target audience more efficiently and cost-

effectively and thus achieve a greater return on their investment. As a result, SMEs can now reach their target audiences more efficiently and compete with and challenge much larger, more established businesses, more effectively, including in concentrated industries. This democratisation of advertising generates additional benefits in the form of greater choice and innovation for customers. Facebook commissioned a study by Copenhagen Economics which surveyed 7,000 businesses across Europe. Businesses surveyed emphasised the importance of technology in helping them reach markets abroad and, in particular, the contribution of Facebook to the growth of European businesses. Facebook's services helped these businesses generate over 98 billion euros in exports last year.

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

Online intermediaries provide small businesses with a reach that would be unthinkable in the offline world and they do so at minimal comparative cost. Facebook also provides these businesses with a variety of free tools that help them benefit from this enormous reach by appropriately targeting the right audience and understanding its engagement, all of which promote the success of these businesses in the digital space, such as Facebook insights. Users derive value from Facebook services and also innovate on the platform creating community value with creative uses of Facebook organisation and fundraising tools. More generally, there is a possibility of negative consumer outcomes if any player in the online ecosystem lacks transparency in its terms and conditions or business processes or if it fails to adhere to the required privacy and integrity standards.

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

We do not think it's necessary or appropriate to include any regulatory proposals with regards to the media sector. We think that business model innovation, rather than regulatory intervention is the most appropriate way to ensure media pluralism and social media is helpful in this regard. The 2017 Reuters Institute Digital News Report found that users of social media are engaged with more online news brands: "indeed when we count the number of brands, we find that on average social media users access more brands (4.34 per week) than non-users (3.10 per week)". As well as increasing engagement with more brands, we continue to expand

our collaboration with the media sector, we recently announced (25th August 2020) that we are expanding Facebook News, which is a personalised destination for news within Facebook. We are working with publishers to bring new news experiences to more countries, and we will pay for news to be available to people in these products. We've identified several countries that we'll focus on bringing the Facebook News product to in the coming year and expect to have multiple countries launch within six months. In order to bring Facebook News to more places, it is critical that regulatory environments invite this kind of investment and innovation. Innovation is critical to building a sustainable news ecosystem. We will keep building new products and making global investments to help the news industry build long-lasting business models.

3. 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
- ❑ **X I disagree to a certain extent**
- ❑ I disagree
- ❑ I don't know

2 **Please explain**
3000 character(s) maximum

It should be clear what the aim and the scope of any regulatory proposal is, all businesses rely on predictable and efficient regulatory oversight that is aimed at remedying market failures. In the Commission's own inception impact assessment, it noted three specific areas that the proposals would be aiming to resolve - Traditional businesses dependency on large online platforms, difficulties in developing innovative solutions, and entry into adjacent markets by large online platforms. Given the problem statement laid out by the Commission it would be wise to consider any regulatory intervention within the bounds of that problem statement. Having said that, we do call into question the overall validity of the areas defined in the problem statement and would argue that the example of a lack of innovative capacity has its issues rooted in other areas than the platform economy. By their nature online platforms have been one of the most innovative sectors, enabling the growth of millions of businesses across the EU. Equally, the problems faced by some 'traditional businesses' (a term we note does not come with a definition) are often rooted elsewhere than in the business models of online platforms. Overall we believe it is a false paradigm; many businesses and industries which one

may consider traditional, thrive in the current market (vendors restricted to local markets can now reach exponentially more consumers) and are delivering a lot of consumer value, whilst many newer businesses may struggle in the current market. Any proposals need to be wary of becoming unwieldy and lacking focus. If the Commission considers the regulatory proposals as a vehicle for broader social issues there is the risk that the regulatory intervention becomes extremely broad in its nature; for that there may be more suitable vehicles to address such issues. Given that the categorisation on 'societal and economic effects' is incredibly vague it is a challenge to specify exactly what these would be.

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
- ❑ **X 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

We do not believe a list of behaviours to be prohibited should be the way in which regulatory intervention is considered – lists of prohibited practices risks being a roadblock to the innovation which the Commission's inception impact assessment states it wishes to stimulate. Given that each business and each situation differs – blanket banning of market behaviours risks being inefficient, negatively impacting consumers, and actually risks worsening the problems at hand given that it will render possible new entrants limited in how they can innovatively challenge any incumbent. The platform economy has seen a number of market entries to challenge the incumbent and this dynamic fosters competition and delivers considerable consumer benefit. Such innovation would be put at risk if businesses were possibly pre-emptively restricted in how they could compete in other markets.

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

- ❑ Yes
- ❑ **X 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

The regulatory toolbox should be the result of an assessment of the relevant market failures to be resolved by intervention, which we do not believe the Commission has currently carried out. Current considerations are relying on broad and undefined terms such as 'gatekeepers' and broad unfounded assumptions of market dynamics as the basis for consideration. Notwithstanding the lack of definitional clarity and therefore the inability to properly define the regulatory tools required, we believe any proposal should adhere to currently accepted and tested methods of market intervention which rely on the definition of markets, assessment of market power, and then the consideration of the appropriate remedy to resolve the market failure. Any regulatory process should aim to follow this process and include the relevant safeguards for ensuring that those subject to the regulation have sufficient rights of appeal and due process.

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
- ❑ **X I don't know**

8 **Please explain your reply.**
3000 character(s) maximum

Given that we do not believe prohibition would be a positive development for the market, consequently attempting to then give comments on administrative design in this case is not possible. As a general principle, a dedicated authority guarantees resources and expertise but needs to have properly defined objectives and competences, which should be strictly complementary and not overlapping those of other existing regulatory authorities. Regulatory entities are also meant to cover activities and not specific entities.

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?**

- ❑ **X 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

There are problems, which we have previously stated in our submissions, with a process that chooses not to define a market and therefore does not enable the assessment of companies based on market behaviours and their possible impact on competition in said market. Using broad models of assessment such as size, or number of user's risks creating the wrong and harmful intervention as the parameters for harm are not identified. We believe there can be value in an approach which assesses a defined market, identifies the market problem and as a result applies remedies on a case by case basis to the market players who are in a proven position to be creating the problem. Europe's regulatory track record has shown that market intervention based on an assessment of defined markets and case by case assessment has largely lead to a legally predictable market environment and has helped achieve many of the outcomes that have been lauded as desirable goals for market intervention – An example is the European telecoms markets where the process of market definition, market assessment and the imposition of proportionate remedies (which have to be justified and then periodically reviewed by the regulator) has created outcomes that some would say are positive such as market entry and lower end users prices. The overarching benefit of market assessment and case by case intervention rather than blanket prohibitions, is the ability to target market failures far more efficiently and potentially reduce the welfare loss from the considerable inefficiencies of prohibitions. There is also a clear benefit of being able to measure and assess success (or lack thereof) of any intervention. If a regulator has defined the market and has identified the competition problem, it is possible after remedies have been imposed to assess success or failure. The ability to adapt and evolve remedies over time is essential in markets that exhibit fast paced innovation and constant evolution such as platforms, therefore periodic review of markets is also necessary.

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?**

- ❑ **X Yes**
- ❑ No

12 **Please explain your reply**
3000 character(s) maximum

The design of the institutional mechanisms to oversee and enforce the regulation should be largely responsive to the design of the regulation itself. At this stage it is not possible to define the precise institutional model that we believe would be the most efficient. Facebook is largely agnostic to any specific model that is put in place, but we do believe they should exhibit certain characteristics – The main one being that the regulatory body is able to act as the single regulator across the European Union and be constantly mindful of the desire to create and further enhance a digital single market. The potential inefficiencies of a fragmented model of regulatory oversight should be avoided; any fragmentation risks limiting the market participants from fully engaging in activities in the whole digital single market.

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

The design of the institutional mechanisms to oversee and enforce the regulation should be largely responsive to the design of the regulation itself. At this stage it is not possible to define the precise institutional model that we believe would be the most efficient. Facebook is largely agnostic to any specific model that is put in place, but we do believe they should exhibit certain characteristics – The main one being that the regulatory body is able to act as the single regulator across the European Union and be constantly mindful of the desire to create and further enhance a digital single market. The potential inefficiencies of a fragmented model of regulatory oversight should be avoided; any fragmentation risks limiting the market participants from fully engaging in activities in the whole digital single market.

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

- ❑ At national level
- ❑ At EU level
- ❑ Both at EU and national level.
- ❑ **X 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

The Commission should assess whether other existing regulatory models such as the newly operating P2B regulation are having the desired effect on the market, and whether or not augmenting those rules could be a more efficient way of achieving policy goals as opposed to a new regulatory regime overall. The EECC as well as the AVMSD are also both pieces of legislation against which the Commission will need to assess the alignment of any new proposals. A balanced assessment would be needed regarding other sector specific rules, especially those that have been designed to operate in a clearly defined and different market such as telecoms, financial services, energy etc. There is a risk of creating inappropriate regulatory interventions if regulatory models are lifted from one industry and placed over another – especially if the regulatory obligations are imposed on markets which lack a clear definition and if a clear competition problem has not been identified.

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

Once again, a clear definition of the market for intervention will be paramount for any proposal. Whilst we do agree that where there is a market failure, which exhibits consumer harm, a regulator should act to reduce consumer harm. We would urge regulators to resist the temptation to propose a "regulation of everything" that aims to resolve highly diverse and largely unrelated policy issues under one proposal. Our belief, and also the Commission's own Inception Impact Assessment has largely drawn on the view that gatekeepers exhibit a level of economic power, (which the Commission eludes to as having negative impacts on a number of players) – As a result of this, if any intervention is to be designed, it would be wise to focus on economic power issues as oppose to a seemingly random collection of policy goals. It is also probable that 'societal' goals may be more efficiently addressed on a standalone basis as opposed to creating catch all policies.

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

Data is available, non-rivalrous and reusable therefore success is determined by the business model and know-how; there are challenges of keeping data private and secure and how large platforms commit to this in all their activities. Data is already flowing from platforms in valuable ways and new value preserving opportunities could be explored that would probably require

some questions being resolved like the ones referenced in our answer to question 2.10, such as the nature of the data to be shared, the protection of data and the rights of the consumer. We are already actively participating and exploring ways in which meaningful data sharing can take place and this an area we will continue to explore and will be keen to be part of any future dialogue on.

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

We do not think it's necessary or appropriate to include any regulatory proposals with regards to the media sector. We think that business model innovation, rather than regulatory intervention is the most appropriate way to ensure media pluralism and social media is helpful in this regard. The 2017 Reuters Institute Digital News Report found that users of social media are engaged with more online news brands: "indeed when we count the number of brands, we find that on average social media users access more brands (4.34 per week) than non-users (3.10 per week)". As well as increasing engagement with more brands, we continue to expand our collaboration with the media sector, we recently announced (25th August 2020) that we are expanding Facebook News, which is a personalised destination for news within Facebook. We are working with publishers to bring new news experiences to more countries, and we will pay for news to be available to people in these products. We've identified several countries that we'll focus on bringing the Facebook News product to in the coming year and expect to have multiple countries launch within six months. In order to bring Facebook News to more places, it is critical that regulatory environments invite this kind of investment and innovation. Innovation is critical to building a sustainable news ecosystem. We will keep building new products and making global investments to help the news industry build long-lasting business models.

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

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

- ❑ **X High level of technical capabilities including data processing, auditing capacities**
- ❑ Cooperation with extra-EU jurisdictions
- ❑ Other

20 **If other, please specify**
3000 character(s) maximum

N/A

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

The role of any proposed regulatory authority will differ based on the design of the regulation it is there to enforce. If the regulation itself is designed in a way which requires consistent monitoring and review, clearly this would lend itself to a relevant staffing to support such functions. If the regulatory authority conversely was monitoring a list of prohibitions, there would need to be a different emphasis placed. Any regulatory authority needs to be an open, and communicative body which would also have the sufficient depth in expertise.

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

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

23 **Other – please list**
3000 character(s) maximum

N/A

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

Clearly a regulatory authority would require a variance in its obligations based on the type of regulatory framework that is ultimately decided – If the role of the authority were to be focused on monitoring for example then that would be the most appropriate and if the authority were to be designated further powers to intervene in the market then perhaps more tools would be appropriate. What would not be appropriate would be an obligation to report into a regulator to announce new possible business decisions. Such an innovation by permission system would have a strongly negative impact on innovation, competition and the overall business environment and would be a step backwards into certain regulatory practices that have long since disappeared from the EU (e.g. tariff notification).

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					X	
2. There is a need for an additional regulatory	X					

framework imposing obligations and prohibitions that are generally applicable to all large online 39 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 caseby-case basis			X			
4. There is a need for a New Competition Tool allowing to	X					

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.	X					

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

The NCT inception impact assessment identifies two types of "structural competition problems" that the Commission's existing enforcement toolkit cannot address:
• "Structural risks for competition" where "certain market characteristics [...] and the conduct of the companies operating in the markets create a threat for competition" (emphasis added), with "tipping markets", "[companies occupying] an entrenched and/or gatekeeper position", and "unilateral strategies by non-dominant companies to monopolise".
• "Structural market failure", such as where a market is "displaying systemic failures going beyond the conduct of a particular company with market power" and "oligopolistic market structures with an increased risk for tacit collusion".
However, insofar as the NCT would apply to unilateral conduct, it is not apparent that there is an "enforcement gap" even if such dynamics were at play. The TFEU gives clear powers to the Commission to take action to tackle two distinct and clearly articulated scenarios. EU competition law today distinguishes between agreements and concerted practices between independent undertakings, which may be caught by Article 101 TFEU, and unilateral conduct which may be caught by Article 102 TFEU. The European Courts have consistently held that unilateral conduct only falls within the scope of EU competition law if the company at issue is

dominant. To date, there has been no evidence-based claim that the Treaty leaves a meaningful "enforcement gap" with respect to anti- competitive unilateral conduct. The NCT IIA explains that the NCT is "complementary to the Commission's new initiative on platform- specific ex ante regulation, which seeks to provide a fair trading environment for the platform ecosystems". Although purportedly "complementary", the Commission's ex ante regulation and NCT projects appear substantially similar. The envisaged ex ante regulatory instrument would specifically target "large online platforms" deemed to be "acting as gatekeepers" benefitting from "significant network effects". The NCT, similarly, identifies market positions of "entrenched dominance", "gatekeeper position[s]" and "network and scale effects" among the structural competition problems meriting application of the tool. Yet while the scope of these partially duplicative initiatives is not conclusively determined, the Commission has already resolved that they will be administered by different Directorates- General (CNECT and COMP, respectively). The parallel proposals therefore create a risk of a lack of clarity as to competence, inconsistent enforcement, and a duplicative compliance burden for the businesses concerned.

27 **Are there other points you would like to raise?**
3000 character(s) maximum

No

ONLINE ADVERTISING

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

On Facebook, people can also easily access information about how ads work on Facebook, why they are shown certain ads, specify that they no longer want to see ads from a certain advertiser with one click, and adjust the information that is shared with advertisers via our "Why am I seeing this ad?" and Ad Preferences tools. Although people can't opt out of seeing ads entirely, each Facebook user can influence the types of ads they see by giving Facebook feedback or hiding ads and advertisers that they don't want to see.

11 **Do you publish or share with researchers, authorities or other third parties detailed data on the advertisements published, their sponsors and viewership rates? Please explain.**
3000 character(s) maximum

Facebook launched the Ad Library, which provides advertising transparency by offering a comprehensive, searchable collection of all currently active ads running across Facebook apps and services, including Instagram. People are able, at minimum, to view the content of all ads.

When it comes to political advertising, a deeper level of ad transparency is necessary to ensure voters are aware of who seeks to influence their views and make campaigns accountable for their messaging. This additional level of transparency can include:

- Identification of the sponsors within the advertisement;
- Registration and/or pre-approval of authorizers or sponsors with a regulator; and
- Archiving of political advertisements

Political ads are then archived in the Ad Library for 7 years. This archive offers a range of additional information that shows what other ads political campaigns are running, including

who paid for them, where they ran, and information on who the ads have reached. (For more information on Ad Library and political advertising policy, see here.)

We have expanded access to our Ad Library API for others to analyse ads related to politics or issues. Our identity confirmation process helps us make sure people are who they say they are, and can take up to a few weeks.

Another way we share data with researchers is our partnership with Social Science One. It implements a new type of partnership between academic researchers and private industry to advance the goals of social science in understanding and solving society's greatest challenges. When researchers want to study Facebook's data through the programme, they are invited to apply for access to data via the Request for Proposals Section under the Facebook Partnership section of the Social Science One website.

For additional information, please see our response to Section 4, Questions 18- 21 of this consultation.

12 **What systems do you have in place for detecting illicit offerings in the advertisements you intermediate?**
3000 character(s) maximum

Advertisers are required to comply with our Advertising Policies. These policies augment our Community Standards and set out additional rules governing paid ads on our platform. Among other things, they restrict or prohibit the promotion of certain types of goods and services, including those that may carry higher risk of illicitness, for example, tobacco and e-cigarettes, weapons, drugs, and adult products and services, among others. Our policies also specifically prohibit offering of goods that violate the intellectual property rights of third parties such as counterfeits.

All ads are subject to our ad review system, which relies primarily on automated tools, including machine learning classifiers that are trained to identify signals or patterns, to check for certain types of violations of these policies. This review happens automatically before ads begin running, but Facebook may also re-review ads after they're live, for example, based on feedback or reports from users.

Ads are made up of several components, such as images, video, text, and targeting information, and each of these is reviewed by the ad review system for various types of violations. The ad review process may also extend to an ad's associated landing page or other destination (such as apps).

If a violation is found at any point in the review process, the ad will be rejected. Additionally, violations of our terms and policies may result in further enforcement actions, including against associated assets like ad accounts, Pages, business managers, and users.

In addition, illicit offerings may be detected via reports from governments, trusted flaggers, consumer and advertising authorities, and law enforcement through established, dedicated channels.

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

We have absolutely no desire to profit from illegal content or goods. Our Community Standards are what keeps our platforms safe. We have over 20 areas of detailed policies that outline what is and what is not allowed on Facebook from a content perspective. We also publish regular reports to give our community visibility into how we enforce policies, respond to data requests and protect intellectual property, while monitoring dynamics that limit access to Facebook products.

For contextual placements like Instant Articles, in-stream video, and Audience Network, we offer tools to prevent ads appearing in content that does not align with their brand: block lists, inventory filters, content whitelists, and live stream exclusions. We also take steps to help advertisers understand how their ads show up on our services, and to provide refunds in certain circumstances. For example, we have built a Brand Safety Controls interface where advertisers can review publishers, individual in-stream videos, and Instant Articles in which their ads may appear in. And we refund advertisers when ads run in videos or Instant Articles that are determined to violate our network policies.

15 **From your perspective, what measures would lead to meaningful transparency in the ad placement process?**
3000 character(s) maximum

People should be able to tell who the advertiser is and see the ads they're running. This is why we have introduced Page Transparency and the Ad Library. People can go to any Page on Facebook or visit the Ad Library to see all active ads - both political and non-political - any

advertiser is running, and we require that all ads be associated with a Page as part of the ad creation process. While platforms can build systems that allow advertisers to accurately disclose required information, the primary onus for providing accurate information should be on advertisers given the scale and volume of online political advertising and platforms' limited ability to verify off-platform and offline information. Platforms like Facebook can restrict the ability of an individual that we catch providing a false ID from using our services. But this is minor compared to the types of sanctions only governments can do, like disqualify someone from an election or impose criminal or civil penalties.

16 **What information about ads displayed online should be made publicly available?**
3000 character(s) maximum

First and foremost, people should be given information about the ads they see, especially for political ads, and the page running them. This is why we have introduced Page Transparency and the Ad Library. People can go to any Page on Facebook and Instagram or visit the Ad Library to see all active ads - both political and non-political - an advertiser is running, and we require that all ads be associated with a Page as part of the ad creation process.

On Facebook, people can also easily access information about why they are shown certain ads, specify that they no longer want to see ads from a certain advertiser with one click, and adjust the information that is shared with advertisers via our “Why am I seeing this ad?” and Ad Preferences tools.

It is also important to provide transparency on what is in the advertising ecosystem to help hold advertisers more accountable. This is why Facebook launched the Ad Library, which provides advertising transparency by offering a comprehensive, searchable collection of all currently active ads running across Facebook apps and services, including Instagram. People are able, at minimum, to view the content of these ads.

When it comes to social issues, electoral and political advertising, a deeper level of ad transparency is necessary to ensure voters are aware of who seeks to influence their views and make campaigns accountable for their messaging. This additional level of transparency can include:

- Identification of the person or entity responsible for the advertisement
- Registration and/or pre-approval of the advertising entity by a regulator. At Facebook, we require the Page admin of advertisers running political ads in the EU to confirm their identity.

- Archiving of political advertisements, such as Facebook's Ad Library which houses ads in the EU about social issues, elections and politics for a period of 7 years.

When Facebook identifies an ad that falls within our definition of political advertising - i.e. "ads about social issues, elections or politics" - we require the individual running such an ad to confirm their identity by submitting identification document(s) issued by the country where they want to run the ad. We also require political advertisers to insert a "paid for by" disclaimer either on or alongside each advertisement so that anyone who views it can see the sponsor of the ad. The disclaimer may include more information about the "paid for by" entity, such as the organisation's email address, website, phone number and physical address.

Political ads are then archived in the Ad Library for 7 years. This archive offers a range of additional information that shows what other ads political campaigns are running, including who paid for them, where they ran, and information on who the ads have reached. (For more information on Ad Library and political advertising policy, see here.)

While platforms can build systems that allow for accurate disclosure of required information, the primary onus for providing accurate information should be on advertisers given the scale and volume of online political advertising and platforms' limited ability to verify off-platform and offline information. Platforms like Facebook can restrict the ability of an individual that we catch providing a false ID from using our services. But this is minor compared to the types of sanctions only governments can do, like disqualify someone from an election or impose criminal or civil penalties.

17 **Based on your expertise, which effective and proportionate auditing systems could bring meaningful accountability in the ad placement system?**
3000 character(s) maximum

Rather than an audit of the ad placement system, we believe meaningful accountability comes from a holistic look at a platform's overall content moderation system. In order to meaningfully audit platforms' systems, widely agreed global standards against which platforms can be evaluated are needed. Currently, none exist, so a first step would be to formulate such standards. These standards should ideally be formulated based on industry expertise, but with broad buy-in from global regulators, academics, and civil society to minimize fragmentation of oversight and multiple conflicting standards.

Collaborating Across Industry

We are collaborating with industry partners to make online platforms safer for businesses and people. Our work with partners includes:

- Participating in the World Federation of Advertiser's Global Alliance for Responsible Media (GARM) to align on brand safety best practices, scaling education, common tools and systems, and independent oversight for the industry, as well as identify actions that will better protect consumers online.
- Certification from independent groups, like the Digital Trading Standards Group which specifically examines our advertising processes against JICWEBS' Good Practice Principles and is a requirement for achieving the Interactive Advertising Bureau's Gold Standard.

Searchable Ad Database
Finally, a public, searchable database of ads allows journalists, regulators, watchdog groups, researchers, academics and people in general to hold advertisers accountable. At Facebook, this has been offered in the form of the Ad Library.

To help people scrutinize the ads in the advertising ecosystem, the Ad Library provides a comprehensive, searchable collection of all currently active ads (political and non-political) running across Facebook apps and services; an archive of political ads that remain in the library for 7 years; and aggregated insights. We have made several updates to these tools since they were first launched. As we continue to receive feedback about these tools, we will make improvements to make it more insightful to people.

18 **What is, from your perspective, a functional definition of 'political advertising'? Are you aware of any specific obligations attaching to 'political advertising' at a European or national level?**
3000 character(s) maximum

Regulators must address the threshold question of what makes an advertisement "political". Is it just when an advertisement mentions or features a candidate or a ballot measure? Does it matter who paid for the ad? What about social issues that are associated with a particular candidate or party? And how is that list of issues defined?

Which definition a government regulator prefers may depend on the outcome they are trying to achieve. For example, if a government chose to implement a blackout period that would forbid any "political ads" for a certain period of time ahead of an election, it may opt for a narrow definition, to avoid banning ads dealing with advocacy on social issues. Other

governments may prefer a broader definition to ensure the transparency of any paid content that might be relevant to an electoral outcome.

In the EU, there is a patchwork of definitions for political advertising that makes consistency across platforms and across countries a challenge. In Germany, for example, the upcoming Interstate Media Treaty will oblige online advertisers who wish to run ads of political, religious or ideological nature to provide transparency on who they are in an appropriate manner. However, it is unclear what would make an ad “political, religious or ideological” in nature. For example, would an ad providing information about a religious service fall under the definition?

In France, the law against the manipulation of information requires large-scale online platforms to provide users with “honest, clear and transparent information” about the identity and corporate purpose of anyone who paid to promote informational content related to a “debate of national interest” during an election campaign period.

- We have taken a broad definition for ‘political advertising’ and adopted a policy that applies to all “ads about social issues, elections or politics” so that transparency obligations and other requirements can be imposed on a broad category of ads that could influence political discourse. Any advertiser who wants to create or edit ads in the European Union that reference political figures, political parties, elections in the EU (including "get out the vote" campaigns) or social issues within the EU (civil and social rights, crime, economy, environmental politics, immigration, health, political values and governance, and security and foreign policy) will be required to go through the authorisation process and have a "Paid for by label."

There is also the question of “foreign” actors. Governments that have electoral rules in place would usually make distinctions between citizens and foreign actors, recognizing that inherent rights of a foreign individual to engage in the political debate are reduced. However, in today’s world of borderless online communication, these lines are increasingly blurred. Individuals can follow, comment on, and participate in the political processes of countries across the globe. But when it comes to political advertising, should they be allowed to do the same?

In the EU, there is the added complexity of the Member States. How should citizens of another Member State be treated? Should they be treated as a foreign actor? Would it be considered interference if a citizen or government of one Member State runs ad campaigns to influence the outcome of an election in another EU country? Furthermore, electoral laws in the EU are determined and enforced at the national level, for both the European and national elections. Election regulators typically have little or no ability to enforce against

anyone who is outside their jurisdiction. If people are allowed in other EU countries to run political ads, then there may not be an effective way for the local election regulator in any particular country to enforce against these campaigns, especially within the short time frame of the election period.

Finally, the primary onus for providing accurate information should be on advertisers given the scale and volume of online political advertising and platforms' limited ability to verify off-platform and offline information.

A functional definition of 'political advertising' for the EU will need to try to answer all of these questions.

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

Facebook has set a new standard for transparency in digital advertising with our Ad Library, which provides a comprehensive, searchable collection of all active and inactive social issue, electoral and political ads. The Ad library provides users with a substantial amount of information, including the "Paid for by" entity behind a political ad and information about that entity, such as the website, email address and telephone number.

However, setting transparency standards for advertising should not be left in the hand of one or a handful of companies. Legislation should be updated to set standards for the whole industry and answer questions like, should all online political advertising be recorded in a public archive similar to our Ad Library and should that extend to traditional platforms like billboards, leaflets and direct mail? Questions around what constitutes a political ad, who can run them and when, what steps those who purchase political ads must take, how much they can spend on them and whether there should be any rules on what they can and can't say – these are all matters that can only be properly decided by legislators and regulators.

The primary onus for providing accurate information should be on advertisers given the scale and volume of online political advertising and platforms' limited ability to verify off-platform and offline information.

Aside from disclosure measures to bring more transparency into the political advertising space, there are also authenticity measures that can help enhance the information that is being made transparent. For political ads, Facebook requires advertisers to confirm their

identity by providing a copy of their ID as well as include a disclaimer with information about the “Paid for by” entity. The disclaimer information could be further authenticated if there were an official or authoritative source, such as a business or campaigners register, that we can verify against to make sure the “Paid for by” entity is legitimate. This will make it even harder for advertisers to mislead people about who they are.

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

Facebook has an integrated business model by which we connect advertisers and publishers, as a rule, with no intermediation. This allows Facebook to have clear visibility on the entire value chain as, otherwise than in the Adtech space, there's no multitude of intermediaries at each level of the chain. This allows us to provide a high level of transparency.

Facebook has devoted significant efforts to empowering advertisers through use of its tools and analytics to measure and manage performance of ads in real-time using its ads reporting metrics, insights metrics and conversion. For example, Facebook is enabling advertisers to move away from ‘final click’ metrics towards multi-touch attribution systems in order to create better advertising campaigns and assess effectiveness of advertising campaigns more accurately.

These advertiser metrics can be accessed through Facebook’s self-service tools – such as Ads Manager, Brand Lift, and Conversion Lift – all of which are regularly updated to reflect the expectations of advertisers. For example, in October 2018, Facebook introduced Facebook Attribution to provide marketers with a more holistic view of the complex customer journey both on and off Facebook, providing measurement of the impact of ads across Facebook family applications and services and across publishers.

Facebook engages with over 40 third-party measurement companies and entities worldwide to provide advertisers with independent metrics and comparisons, as well as third parties who perform regular checks on Facebook’s ad viewability and other attention metrics. In line with Facebook’s goal to improve transparency for users of its platform, Facebook would welcome a discussion on how to improve standards in cross-platform measurement and third-party verification in order to enable advertisers to effectively measure the success of their campaigns across different advertising media, including online and offline channels.

21 **Are there other emerging issues in the space of online advertising you would like to flag?**
3000 character(s) maximum

The most significant emerging issue in relation to online advertising is in relation to political ads. We have set out in Question 19 how we ensure accountability with advertising.

Single country vs. cross-border advertising
One of the key issues identified during the European elections in 2019 is the need for a common regulatory framework across the EU for political advertising. To hold advertisers accountable across the EU is a highly complex task, given the variety of political systems, national electoral regulations and the number of local, regional, and national elections (each with its own complexity) that are taking place in EU countries throughout the year. Adding to this complexity is the European elections that run across all EU member states every five years.

Electoral laws in the EU are determined and enforced at the national level, for both the European and national elections. Election regulators typically have little or no ability to enforce against anyone who is outside their jurisdiction. If people are allowed in other countries to run political ads, then there may not be an effective way for the local election regulator in any particular country to enforce against these campaigns, especially within the short time frame of the election period.

We had designed our ad transparency policies to mitigate the risk of foreign interference, by requiring advertisers to fulfill specific identity confirmation and disclaimer requirements for each country they would like to target, in doing so we have taken into account local frameworks. Therefore, an organisation that would like to advertise in multiple EU countries would need to have a local representative complete the ad authorisation requirements for each of those countries. During the European elections, this process frustrated advertisers who wanted to run pan-EU political ad campaigns but did not have the structure in place to meet the single-country ad authorisation process.

The question about “foreign” actors also needs to be considered in this respect. In the EU, some countries have electoral rules that make distinctions between citizens and foreign actors, recognising that inherent rights of a foreign individual to engage in the political debate are reduced, which may include rules banning foreign donations (including in-kind donations such as funding of ad campaigns), to political parties and candidates. If foreign actors have less rights to engage in the political debate of another country, how would “foreign” in the context of the EU be measured? Would people or governments from one EU country campaigning in another EU country’s election be considered “foreign”? Would it be

considered interference if a citizen or government of one Member State runs ad campaigns to influence the outcome of an election in another EU country?

GOVERNANCE AND ENFORCEMENT

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 a/several 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					5	
Requirements to have a legal					5	

representative or an establishment in more than one Member State						
Different procedures and points of contact for obligations to cooperate with authorities					5	
Other types of legal requirements. Please specify below						

5 **Please specify**
3000 character(s) maximum

As noted in the table above, most of the obligations mentioned represent burdens for companies trying to expand their digital services across EU Member States.

First of all, having different processes and obligations imposed by Member States and various procedures and points of contacts with authorities is extremely inefficient. Currently, there are different obligations and processes for noticing, detecting and removing illegal content across EU Member States. While Facebook has robust and efficient procedures, including a dedicated channel used by multiple partners in every Member State to request take downs of content considered locally illegal, making assessments according to several different countries' laws can be extremely challenging.

Regulation should reflect the way an internal market operates for digital services (i.e., on a pan-European basis). For this reason, we support the opportunity provided by the DSA to harmonise rules at EU level.

Whilst we are aware of the difficulty of harmonizing the criminal system, it is extremely important for definitions and regulations to be harmonised across different types of illegal content, for example terrorist content. For this reason, we welcome the efforts being made to create a harmonised system in the draft Terrorist Content Online Regulation.

Apart from the importance of consistent legislation with regards to definitions, we also note that having a dedicated regulatory point of contact or clearly explained, straight-forward

procedures for cooperation with authorities for specific issues would create efficiencies. While certain types of content may require specific approaches, processes and obligations should be as aligned as possible; this would reduce frictions and increase the ability to act expeditiously. There is a risk that protections are decreased if there are different processes for each type of illegal content, or between Member States.

Additionally, we also find that a requirement to have a legal representative established in more than one Member State would be burdensome and run contrary to the Freedom of Establishment as set out in Art. 49 in the TFEU. Such a requirement is also an unnecessary construct in the current times. Work habits are changing and the future of work definitely envisages more remote working. The recent COVID19 outbreak has meant that many workers, who were able to, worked from home, and we believe this will continue and result in more flexible working arrangements. This makes respecting the principles of Freedom of Establishment even more important.

The nature of a global service means that the offering is the same across the EU, with the same policies, processes and procedures. This allows for a company to invest in improving the effectiveness of process systems, to deal with illegal content efficiently, and keeps agility in the market. Lack of harmonisation of processes and procedures results in challenges in training of staff, who have to then manage different interpretations of what is sometimes the same content and creates the opportunity for error due to lack of EU-wide definition. Harmonized rules and processes would also lower the regulatory burden on smaller players or new market entrants.

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

- ❑ **X Yes**
- ❑ No
- ❑ I don't know

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

3000 character(s) maximum

Facebook is subject to several national enforcement measures coming from EU Member States other than its country of establishment.

In Germany, social network providers are subject to the Network Enforcement Act (NetzDG). Under NetzDG, companies are obliged to offer users a reporting channel for content violating certain crimes from the German criminal code, such as incitement to hatred and defamation, and - upon receipt of such reports - remove the content in question within short time frames. These time frames are set between 24 hours and 7 days from receipt of the report depending on the kind of content. In order to comply with NetzDG, Facebook has created a dedicated reporting form[5]. Companies are further required to report extensively and regularly - twice a year - on their compliance with this law and statistical data such as reporting volumes and must appoint national representatives for (i) legal service of certain documents and (ii) as a point of contact for requests from law enforcement authorities.

From April 2019, a Bill on the Fight Against the Manipulation of Information in France came into force. According to the bill, online platforms are obliged to provide the user with "information that is fair, clear and transparent" on the identity of the advertiser and the amounts spent on sponsored content that relates to a debate of public interest. The bill also requires companies to have an easy and transparent system enabling users to report false news and send yearly reports to the French media authority (CSA) about their efforts to fight the manipulation of information on their services.
Facebook submitted its first report to the CSA at the beginning of April 2020. Facebook extensively archived, our Ad Library to meet the French legal requirements and we have had regular discussions with the French regulator on the measures we have taken to combat misinformation during the COVID-19 crisis.

The examples mentioned above represent fragmentation of the EU single market and we are noting more initiatives of this kind springing up at national level in Austria, Ireland and Spain, to name a few. Additionally, in Germany, the 'NetzDG' is being further updated, with additional measures being added to the original law and the country has incoming Youth Protection and general Media Regulation legislation that go beyond AVMSD and in large part ignores the country of origin principle.

If every single EU Member State created their own slightly different "NetzDG", imposing different product solutions on digital services providers, it would be extremely burdensome for companies wanting to offer their services across the EU.

In addition, Turkey (a candidate country for EU Membership) has introduced new regulations which raises concerns about suppression of free speech and freedom of expression (as this regulation concerns both illegal and harmful but legal content) and could influence some administrations to follow similar approaches.

5 (this form is geolocated to Germany)

As mentioned in our answer to question 5, having different obligations and uncoordinated enforcement measures imposed by different Member States is inefficient and counter-intuitive. Digital services are cross-border in nature, and users are based across Member States. Forcing companies to divert resources to create bespoke variants of their services for each country also risks distracting them from managing the potential harm at scale. Fragmentation of the regulatory regime would also create a barrier to entry to the EU market, stifling European innovation and resulting in an unsatisfactory user experience for European users.
We support as much harmonisation of the rules at EU level as is possible, which will significantly improve the legal certainty, and would also strongly recommend introducing robust coordination between Member States.

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

- ❑ Yes
- ❑ **X No**
- ❑ I don't know

9 **Please explain**
3000 character(s) maximum

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

The most important factor for robust regulation is for a platform to have a single set of rules harmonised as much as possible, managed through a single regulator, avoiding divergences of rules across platforms. There are a number of ways this can be achieved, and it could include some mechanism or body for Member States Regulators to coordinate and cooperate and one regulator to manage the regulation of the platform.

Having the rules about content harmonised as much as possible would help to ensure a common understanding of the key principles with regard to the provision of digital services across the EU, in particular in relation to definitions of illegal and harmful content and any regulatory standards, regulations or rules that might be applied. It would need to curb - as

much as possible - divergence of legal systems and interpretation across Member States, which would undermine the realisation of the single market and it would ensure similar protection is provided to all EU citizens regardless of which country the digital services they are using are based. The DSA should indicate the processes, whilst providing safeguards and flexibility, and should not be so restrictive as to dictate how these systems should look or operate. Any compliance in relation to the rules should be assessed on the basis of the overall effectiveness.

A situation where cross-border services deal with multiple regulators, and multiple (potentially competing) requirements would inhibit the development and innovation of cross-border services in the EU, and potentially act as a barrier to entry for new actors. It would also create issues for training of staff to manage compliance if there are different and competing regulations, and thus decreasing the effectiveness. This would also create issues for SMEs and a low level of administrative and regulatory hurdles is needed to insure growth and innovation for small businesses.

We support consistency across the different EU instruments covering digital services (such as AVMSD, e-Evidence, etc). The benefits of a consistent and harmonised approach would be to ensure growth for small businesses. The majority of advertisers on Facebook are small businesses, which are growing their businesses in their local areas and beyond. This has generated a clear economic value in Europe, with international sales corresponding to an estimated €208 bln in economic activity and an estimated €98 bln in exports[6]. This ability to scale local businesses digitally cross-border within the EU as well as further afield is essential for European growth and competitiveness, innovation, culture and values. A consistent, harmonised and well-functioning single market is the foundation for businesses' ability to scale, hire more people and become successful - and Facebook has always been supportive of greater integration and removing barriers to growth for small businesses, which is even more important in light of the unprecedented economic shock to the EU economy caused by the Covid-19 pandemic. A stable growth environment is essential for the EU's economic recovery and we see our responsibility in enabling SMEs across Europe to take advantage of digitisation and thrive, as exemplified by the vast array of tools and resources launched to support them during and beyond the crisis. Companies such as Facebook can serve as an effective driver for greater deepening and broadening of the single market and innovation economy for the benefits of SMEs and startups in Europe.

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

[6] Copenhagen Economics. (2020). *Digital Transformation in Business*. Available at: https://www.copenhageneconomics.com/publications/publication/digital-transformation-in-business

- ❑ Significant reduction of turnover
- ❑ Limited reduction of turnover
- ❑ No significant change
- ❑ **X Modest increase in turnover**
- ❑ Significant increase of turnover
- ❑ Other

12 **Please explain**
3000 character(s) maximum

After seeing flat year-over-year revenue growth in the first few weeks of April, we saw a considerable recovery in May and June. Our total ad revenue globally for Q2 was $18.3 billion, which is a 10% year-over-year increase. In Europe, this year-over-year increase was 9%. The earnings data is published on Facebook investor relations website.

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

- ❑ **X Yes**
- ❑ No
- ❑ I don't know

14 **Please explain**
3000 character(s) maximum

Facebook is and has always been supportive of greater Single Market integration. A harmonised and well-functioning Single Market is the foundation for businesses' ability to grow and scale across the EU. This is even more important in light of the economic downturn and impact of COVID-19 on the state of - especially small - businesses and start-ups in the EU. Removing barriers within the Single Market and consistent implementation of EU regulation to create a stable growth environment is essential for the EU's economic recovery. Practical steps have to be taken to close the gaps in the Single Market - this would be the single most important and powerful step in empowering Europe's digital economy.

Companies such as Facebook can serve as an effective driver for greater deepening and broadening of the Single Market. Our services have enabled enterprises of all sizes to run affordable and efficient marketing campaigns across the EU to find new commercial opportunities, scale their business, hire more people and increase cross-border trade. This has generated international sales corresponding to an estimated €208 bln in economic

activity and an estimated €98 bln in exports last year[7]. Our tools also enable businesses to measure their return on investment to ensure they are getting good value, and adjust if not, which is relevant in today's context where even small gains in efficiency can help entrepreneurs stay afloat during an economic downturn. Across the EU, 25 mln businesses, large and small, use our services to generate sales - most of them do so using free tools (example: see here, "*Before Facebook, all of our sales were in Italy. Now, 90% of our sales are abroad*", by Fratelli Saraceni). There are many other online services European businesses can choose, which reflects the vast choice of digital tools businesses have.

Given that Facebook's business model is based on creating value for the many businesses seeking to expand their customer base across borders, we support the Commission's efforts to make the Single Market work for entrepreneurs. European innovators face real difficulties when trying to grow and scale their businesses cross-border, which are likely due to factors such as fragmentation and lack of consistent implementation of EU rules across the bloc, an environment that is not supportive of large scale experimentation, and remaining barriers within the Single Market. As noted by the former Commissioner for the Internal Market Mario Monti: *"I know […] how many violations of those rules are put in place by member states when they try to preserve the national interest and therefore to have the market less single and more fragmented."*[8] Furthermore, as noted in recent Council Conclusions: *"the platform economy is an important part of the Single Market, as it connects European companies and consumers across national borders, enables trade, entrepreneurship and new business models, as well as increases consumer choice of goods and services."*[9] This is precisely what Facebook wants to support. We offer the possibility to all players in the economy to scale up, access cutting edge innovation, and maximise the opportunities that are available in the Single Market. As such, we remain fully supportive of any attempts to eliminate barriers to make the Single Market a reality and stand ready to help.

The following questions are targeted at all respondents.

1 **Based on your own experience, how would you assess the cooperation in the Single Market between authorities entrusted to supervise digital services?**
5000 character(s) maximum

[7] Copenhagen Economics. (2020). *Digital Transformation in Business*. Available at: https://www.copenhageneconomics.com/publications/publication/digital-transformation-in-business

[8] "*Don't blame Brussels: Mario Monti weighs into clash over EU champions"*. Appeared in Politico on 11 February, 2020: https://pro.politico.eu/news/mario-monti-dont-blame-brussels-mario-monti-weighs-into-clash-over-eu-champions

[9] Council Conclusions from 9 June 2020 on *Shaping Europe's Digital Future*, para. 47. Available at: https://eu2020.hr/Home/DocumentDownload/244

At a national level, in the EU, there are a number of rules and regulations in place and we note that there is currently a risk of having different regulatory regimes on similar issues, and a risk that the approaches taken may not have coherence with each other. Our experience is that there is little coordination within the single market, which creates market fragmentation. There are already issues of having to manage enquiries and requirements from multiple regulators without formal jurisdiction, that imposes not only a heavy burden (for example with take down notices or litigation), but also creates the risk of having competing requirements in neighbouring countries. For instance, Facebook has a dedicated channel for government partners to request take downs of content that violates our community standards, policies or local laws, the Government Casework Channel, which is used by multiple partners in the Member States. Facebook also has a specific channel (known as the Consumer Policy Channel) for ingesting reports of content or activity on Facebook that is commercial in nature and believed to be locally unlawful or in violation of an applicable policy. The channel is currently used by partners (which includes a range of government/regulatory, quasi-regulatory and self-regulatory bodies) across nearly all Member States. Facebook believes these channels would be made more effective if the requests came via a single source or point of contact. Having multiple channels and multiple authorities involved creates issues of duplication of effort and potentially makes the process less rather than more able to react in a timely manner.

The fragmentation and multiple regulators also reduce the possibility for healthy competition and new entrants within the market, as innovation and economic participation is restricted when there are disproportionate regulatory burdens. Facebook considers that there should be proportionality, which should be assessed according to the characteristics and nature of the service and the risk that is posed. The wrong incentives could discourage growth and diversification if growth would mean regulatory burdens. The essence of a cross-border service requires harmonised cross-border regulation. This fragmentation creates potential for confusion; in regulatory terms by having competing regulations within the EU.

There is further uncertainty when countries implement rules without a harmonised model/ Hypothetically and for example, in the future the actions by the NetzDG regulator BFJ (Bundesamt für Justiz) might conflict with a European regulator's views. The general problem is that the German NetzDG and other German pieces of media legislation (e.g. the Interstate Media Treaty and upcoming youth protection legislation) which will soon come into force do not respect the country of origin principle. For example; the new AVMSD which includes an obligation for video-sharing services to offer a reporting mechanism. The amendments to the NetzDG include this obligation for services that are both social networks and video-sharing platform services. It is already unclear what the situation will be if Facebook's video-sharing platform services (as determined under the Irish implementation of AVMSD) are also deemed to be social networks under German law (or another category of regulated service in another

Member State) as the requirements for each legal framework are not harmonised.This is a difficult question which demonstrates how important a coherent legal framework across the EU is.

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, on a scale of 1 (not at all important) to 5 (very important), each of the following elements.

	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				4		
Cooperation mechanism within Member States across different competent authorities responsible for				4		

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					**5**	
Coordination and technical assistance at EU level					5	
An EU-level authority					**5**	
Cooperation schemes with third parties					5	

such as civil society organisations and academics for specific inquiries and oversight						
Other: please specify in the text box below						

3 **Please explain**
5000 character(s) maximum

As outlined in the questions above, an important factor for robust regulation is for a platform to have a single set of rules managed and consistently applied through a single regulator. There are a number of ways this can be achieved, but it should include some mechanism or body for EU Regulators to coordinate and cooperate and one regulator to be the single point of contact for the platform. This would increase legal certainty by providing guidance to consumers and companies, help the latter take reasonable, feasible, and proportionate measures and ensure protection of fundamental rights. Whilst it's clear that the oversight mechanism should not interfere with responsibilities within the jurisdiction of the Courts, it is important to ensure that harmonised EU legislation and clear directions with regard to implementation should seek to avoid inconsistent positions in the national courts.

A situation where online platforms companies that provide cross-border European wide services face different regulatory requirements imposed by different National Regulatory Authorities (NRAs) in EU Member States risks undermining the fundamental goals of the Digital Single Market. To avoid market fragmentation of online services, any regulatory requirement that is set needs to be consistent across the internal market. Harmonisation of illegal content regulations across the EU would prevent forum-shopping and improve the effectiveness of regulation by ensuring that platforms are not having to manage competing requirements from multiple regulators.

A system whereby platforms are subject to a number of national regulators enforcing diverging legal systems would not only raise the risk of inconsistency and legal uncertainty but would serve as a market barrier to new entrants to the market.

Whilst a cross-border service necessitates the need for regulatory harmonisation, Facebook anticipates that there should be an effective cooperation mechanism to allow for Member States to cooperate on cross-sectoral issues as well as issues that arise between Member States.

There are existing models for this, such as ERGA, EDPB and BEREC. The ERGA model relies on country of origin application of AVMSD rules and works in a context of a lower level of harmonization when compared to the telecom markets, where rules are more harmonized and BEREC has a much more formal statutory role provided by the EECC and institutional setting, supported by an EU Office. In respect to the table above relating to the coordination and technical assistance we have understood this to mean this type of existing model.

Any EU oversight model will in any case require an EU system with strong powers to harmonize the implementation of content regulation requirements across Member States and enough resources to fulfill its duties as a forum for Member State cooperation.

This could be combined with a separate co-regulatory model to tackle harmful content outside of the DSA, the AVMS can be a model of potential framework for both illegal and harmful content. The Oberaxe approach in Spain for managing hate speech is another good example of a co-regulatory model, which ensures that both enforcement agencies and civil society use the same process for reporting, friction is reduced and efficiencies are gained.

The regulator then needs to have clearly assigned roles for supervising the process systems that online platforms put into place for their community guidelines.

Internet companies should be held accountable for the systematic effectiveness of their process systems, rather than holding them liable for each individual piece of content. Any systematic regulation should not be so prescriptive as to set the processes for the platform. While one-off events or individual pieces of content will test the effectiveness of the process, one-off events should not be the focus when it comes to assessing compliance. Any system that looks at holding a platform to account for the systematic effectiveness of the process systems, as defined by harmonised rules that define harmful and illegal content, would also need to recognise that Facebook is and would be also held accountable for specific illegal content via the limited liability regime based upon the notice and take-down regime, which is discussed further in Section 2 of this response.

Cooperation is needed between Member States when such one-off events take place to help form guidance on best practice for such systems. The regulatory model would then be driven by a focus on best practice - not simply compliance. Therefore, incentives for investment in best practice systems should be a key feature of any governance.

To address the final issues raised in question 2 above, whilst Facebook understands the desire for social researchers and other civil society to be able to address specific inquiries , there are a number of potential concerns with such access and it would be desirable to have this coordinated through a voluntary cooperation scheme. It is important that such requests should have a defined and reasoned base or outcome, underpinned by the need for good regulatory outcomes. Of particular concern is the risk of bad actors gaming the platforms once the information from researchers and civil society becomes available. Additionally, there are potential business confidentiality, security, user privacy and competition concerns with interrogation of systems by third parties. There are specific data security risks that are involved with sharing datasets with third parties - not just GDPR but the security risks that may arise from sharing business data, but also information such as how our AI algorithms work, which could be used to bad actors to learn how to circumvent our safety/integrity etc. Further detail relating to concerns can be found in the Q18 in Section 1.2 above

It is also essential to recognise that transparency and explainability may vary from product to product and from one platform to another. Any such system needs to be future proofed to ensure that products and platforms can evolve and drive growth within a flexible system of regulation. The challenge is to design a system that is flexible and responsive to the evolving nature of products and services, as product features continue to evolve as well as consulting with all parties the reporting requirements so they can be built into the system to ensure that it meets good regulatory outcomes.

4 **What information should competent authorities make publicly available about their supervisory and enforcement activity?**
3000 character(s) maximum

There is a need for public authorities to make enough information available to ensure they are held accountable to their citizens, but not so much information as to disclose company confidential information which could create market or competition issues, or information that would allow bad actors to exploit the regulatory structures on the platforms to their advantage.

Any regulatory system should have a requirement to ensure that the regulator is transparent and accountable. This should include transparency in their own processes, including the requirement to consult on procedures for dealing with complaints, investigations and assessment of content moderation systems. Notice when an investigation is started, and

statements of conclusion of investigations and how these conclusions are reached. This should be without interference with the role of the Courts, and should not remove the ability to appeal regulatory decisions.

Transparency for regulators can be achieved also through clearly reasoned removal requests and making data about take down requirement notices, alongside an explanation of the legal basis of this, and action taken on harmful content publicly available. As regulators and social media platforms alike demonstrate a commitment to being transparent and accountable for their decisions, this will facilitate open and critical discussions about how efforts can continually be made to improve protection against both illegal and legal harms.

Many regulators already have within their functioning requirements to ensure that information collected in the course of the regulatory duties are not disclosed without the consent of the business and provisions about the types of information that cannot be disclosed without specific consent of the regulated business, for example business confidential information.

Facebook believes this needs to be ensured as it would allow for reasonable and open dialogue between the parties. So, whilst it is important that any regulatory body is transparent about its activities to citizens, it should not be doing so in a way that would restrict the ability of regulated services to share information about the operation of the service with the regulator. In particular, information that would not be desirable to have in the public domain information that needs to be safeguarded (which could allow appropriation by bad actors or create competition issues).

5 **What capabilities – type of internal expertise, resources etc. - are needed within competent authorities, in order to effectively supervise online platforms?**
3000 character(s) maximum

As outlined in Question 3, Facebook considers it is essential that there is one regulator of contact for services that operate across the whole of the internal market which is accompanied by a strong cooperation body.

Any regulator needs to be structurally, organisationally and financially independent of any government to ensure robustness and lack of political interference in decision making, as is the case with the rules set out in the EECC and the revised AVMSD. This principle should be extended for any further regulatory activity in this area.

Adequate financial and human resources should also be guaranteed by law to ensure that decisions can be made expeditiously. It is worth highlighting the risk that a poorly resourced regulator is likely to take decisions on low-quality evidence that is inconsistent or be so risk-averse that they are rendered unable to make any regulatory decisions.

The regulator needs to fully understand that each platform operates and is built differently but has to comply with a regulatory regime that may not clearly or comfortably fit its structure and operations. In particular, where a law is not built specifically for a platform, this can be extremely difficult (for example, AVMSD is ultimately built for television and OTT audiovisual media services so some of the rules will be difficult to apply to a social network, which does not only have audiovisual content).

Also, a regulator needs to be able to identify how regulatory regimes should be fairly and practically applied to different platforms that are within scope but have different structures and operations. For example, aspects of AVMSD impact both YouTube and Facebook, however, the two platforms operate very differently and have different purposes. A blanket approach for both these platforms will not work.

The regulator needs to be mindful of the practical difficulties that platforms face when implementing measures to comply with different applicable laws and especially if these would affect the user experience. For example, if they are overly prescriptive about the design of how compliance should look.

As the purpose of regulation is to bring good outcomes, it is typically not helpful to set up regulatory bodies that exclusively have fining power (without the option to issue guidance, - binding or non-binding or offer the ability to remedy- instead, or as a first step).

Similar to the AVMSD, any regulatory body should have a function to promote and research media and information literacy. The regulator needs to be empowered to utilise skills that are necessary to fulfil the tasks assigned by Law. A regulator needs a clear and defined ability to delegate functions in certain circumstances, for example if it wishes to utilise skills of co-regulatory organisations, or to seek expertise. Regulation needs to be within the bounds of the regulatory expertise, and not seek to widen the remit. Any regulatory body needs resources to research in order to understand harm and how it is evolving so that decisions and recommendations can be made using an evidence base. Additionally, the skill set needs to have an evolved understanding of the technology used by platforms so that any regulatory recommendations would be based on the technically possible. This could be achieved in the development of regulatory processes to involve early sight of industry and to develop greater partnership with industry to ensure that regulatory solutions are technically deliverable.

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
- ❑ **X Other**
- ❑ I don't know

7 Please explain
3000 character(s) maximum

The DSA must envisage sufficiently strong harmonisation to ensure that legal fragmentation in the EU, and the subsequent damage to the internal market, is avoided.
This would include ensuring that services available within, designed for and actively targeting the EU are subject to the same rules and obligations, regardless of whether their origin is from within the EU or outside
.
In order to determine whether non-EU services fall under the scope of EU law, consideration would need to be given to if a service was designed for or adapted to the EU market.

The cross-border nature of communication is also a defining feature of many internet platforms, so companies tend to see benefit in maintaining one set of global policies rather than country-specific policies that would interfere with that experience. Done well, EU regulations will set the global standard, as observed by the impact of the GDPR. For EU regulation to set the global standard it would need to be applied in a consistent way to all services available to citizens in the EU.

Specific care and attention is needed with regard to exceptions, particularly for third country services. It is likely that a proportion of the services available in the EU that originate from outside will be from a smaller business. Regulations need to be proportionate, according to the characteristics and nature of the service, and level of risk the service poses. Regulatory compliance can be difficult or burdensome when the rules are fragmented, however we would suggest that any exemptions designed to help smaller businesses to flourish would need to be determined very carefully. For example, full exemptions of regulatory requirements to small to medium sized businesses could result in niche services that would have no prospect of significant market impact, becoming the repository of content that would otherwise be removed and subject to regulation on larger services. The regulation

therefore needs to be proportionate to the characteristics and nature of the service, and risk of the company providing a service.

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

Currently there are a number of principles that are set up to ensure the supervision of services established outside of the EU.

The 2000 e-Commerce Directive (ECD) applies to information society services and covers the vast majority of online service providers. It is based on the Country of Origin principle, which allows information society services to provide services across the EU, whilst complying with the laws of the country in which they are established. Within the e-Commerce Directive, a straightforward establishment hierarchy in recital 19 sets out conditions for situations in which there are multiple places of establishment. This is further developed in the revised AVMSD Article 28a, which sets out a series of hierarchies to determine where jurisdiction is applied if there are several subsidiary undertakings within the EU.

The principles of the GDPR, satellite television services under AVMSD and the Copyright Directive apply to services available in the EU regardless if the service provider's place of establishment is outside the EU, and similar principles could be applied here.

The legal framework should ensure that companies can provide services to the EU regardless of their size, reflective of the global nature of services and the internet. The regulations should provide legal and regulatory certainty to online services. Services shouldn't be required to relocate, (but potentially could be encouraged to do so), and although there is no establishment, rules could be created to determine which regulator regulates the service. Some consideration could be given to certain types of services registering with specific regulators for example all non-EU services of a similar type registered with the same regulator, which would allow the regulator to develop expertise in issues related to that type of service and prevent concerns around forum shopping.

The inclusion of such a mechanism would act as an enabler for SMEs and allow for European platforms to grow globally in countries where mutual recognition is applied. Also, as the DSA is more advanced than third country plans for digital regulation, it would encourage third countries to follow a similar model. As with the GDPR, which had success beyond the EU as is an example of an EU regulation that has been widely modelled by third countries the same

could hold true for the DSA, particularly if it included mechanisms of mutual benefit to encourage uptake of the principles in third countries.

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

In any structure, it is very important that the role of the national authority and any coordinating body is clearly defined. Not all aspects of digital regulation will come under the DSA, and not all aspects of the digital services that Facebook provides will come under the scope of regulation. It is very important that the approach is coherent between and across the entire EU acquis. In particular to ensure any implementing legislation remains consistent between Member States. There needs to be a consistent understanding about how platforms are caught / fall within the scope of any regulation (i.e., how different products are categorised as regulated services). Member States (and regulators) should ensure that no product should be subject to two similar but slightly different regulatory regimes Facebook recognises that illegal content is managed in the national courts, however as much as possible there should be alignment on the approach to what is illegal.

As already stated, the service is a single service globally and within the EU, and so having different legal requirements in different Member States creates a range of issues that limit effectiveness in compliance. Having a single regulator to work with, rather than several across Member States will allow for a concerted effort by the platform to comply with regulations, rather than having to manage and understand multiple competing and potentially conflicting requirements. This should be complemented by a strong cooperation body.

There is also a role for coregulatory models, and other forums which create dialogue channels for industry and regulators. Digital services are highly innovative and fast changing. Equally, the challenges that emerge in the digital space can be equally as fast (for example new behaviours by bad actors). Co-regulatory regimes in areas which are still developing, would provide the benefit of being able to be responsive and adaptable (for example in protection of minors mechanisms).

In considering how this might be achieved, it's important when creating a structure to consider what should be avoided. This includes:

- a situation where Member States create rules for anything that isn't explicitly covered by the DSA which would ultimately undermine a structure where there was one

regulator and a cooperation body, as has been observed with the e-Commerce Directive.
- Any inconsistency and inflexibility in the structure.
- Situations where decisions made in one Member State are incompatible with the decisions made in another Member State. For this reason, a strong cooperation body or mechanism is very important, ideally including a mechanism to reach alignment in case of differing views between national regulators before binding decisions are issued.
- Situations where every country has a different material scope of the definition of harmful.
- Giving power to a regulator structure that would allow for arbitrary changes to operations or practices (for example putting limits on end-to-end encryption).

There are a number of ways this might be achieved. It is very important that there is maximum harmonization as much as possible. This would require a bigger role for EU coordination of regulators, to avoid deviation, discrepancies and derogations from the rules. Clearer rules governing the expectations of such a regime. Clear and harmonized definitions, either within the regulation or directive itself or by an EU coordinating body.

Given the dynamic and changing nature of the internet space, there will be an ongoing challenge of needing to design a regulatory system that is flexible and responsive to the evolving nature of the range of products and services in the digital market.

The collaboration could be better than the current systems, with regulators coordinating and working together to define policy, this would provide an opportunity for real collaboration with regulators and governments, rather than a system which is just for check and balances. The role of the coordinating authority would also need clearly defining but could include:

- Defining EU wide policy, in collaboration with Member States and their regulators
- Ensuring approaches within regulatory frameworks are consistent. i.e. they may not all be considering the same issue, but the approach should be the same.
- Establishing clear and harmonised definitions, when they are not defined within the regulations or directive. (when clarification is required)
- Guidelines on harmful but legal content
- Establishing, developing and improving the best of cooperation models and protocols- needs common rules/common standards/common understanding

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

Facebook has had some limited experience of cross-border cooperation of authorities in the specific area of consumer protection. In 2018-19, Facebook (along with Twitter and Google) engaged with the European Commission and the CPC Network of consumer protection authorities to address concerns raised regarding the compliance of social media platforms' terms of service with applicable EU consumer protection laws. This process was instigated pursuant to Regulation 2006/2004. This is an example where a coordinated EU-wide approach was to be welcomed, given the importance of being able to ensure a consistency of approach with regard to platforms' relevant terms and policies across all Member States.

As noted above, having a single regulator to work with, rather than several across Member States, enabled Facebook to agree with relevant CPC Authorities a solution that could be implemented across all Member States without the need for multiple independent national proceedings and avoiding the likelihood of divergent national interpretations of relevant legislation. Overall, therefore, this engagement was constructive and led to a positive outcome for platforms and EU consumers alike.

Nevertheless, this process lacked a clear statutory or procedural framework which led to some uncertainty over:

- The formal scope and legal effect of the cooperation process. In particular, the process did not lead to a formal binding conclusion or approval, leaving platforms with limited assurances that parallel proceedings would not be brought by authorities at a national level that may overlap or conflict with the commitments provided to the CPC Network. Whilst the CPC cooperation procedure has been formalised to some degree by the introduction of Regulation 2017/2394, this is nevertheless a principle that could be borne in mind when comparing this cooperation mechanism in analogous contexts.
- The precise interpretation of relevant legislation, particularly in circumstances where the legislation in question has been interpreted and implemented differently across Member States. For this reason, as noted above, a strong cooperation body or mechanism is very important, ideally including a mechanism to reach alignment in case of differing views between national regulators before binding decisions are issued.

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

The provisions of the Audiovisual Media Services directive that capture video-sharing platforms do not come into force until 19 September 2020, so it may be a little premature to assess if the current system has proven to be sufficient in relation to platforms.

Article 28b offers an appropriate model for ensuring balance, with the focus on the procedural obligations of platform operators.

Audiovisual Media Services Directive is designed to ensure regulatory predictability and certainty. As required under Article 28b(6) of the revised AVMSD, any system should also comply with the requirements of Articles 12 to 15 of the e-Commerce Directive and Article 25 of Directive 2011/93/EU.

As to if the provisions in Articles 3 and 4 would be applicable as a cooperation mechanism for digital services, Facebook would suggest that there is scope for improvement. The cooperation mechanism as set out in AVMSD envisages a system of bilateral cooperation between the Member State where the service originates from and the Member State where the service is targeted. This reflects the nature of audiovisual services, which are adapted and altered for each region. Facebook has the same offering across the EU, and a series of bilateral arrangements envisaged by Articles 3 and 4 of the Directive would be complex and would be challenging to make effective.

The cooperation mechanism needs to reflect this nature of the service, so any cooperation mechanism would need to be in this context. Potentially through a EU cooperation body that looked at cross-border issues as whole, rather than from one territory to another.

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	The provisions in relation to jurisdiction for video-sharing platform services as required by article 28a (7) of the revised AVMSD, are not yet in force. It may therefore be too soon to assess if they should be strengthened. As set out Facebook supports these provisions.
Agreeing on guidance for consistent implementation of rules under the AVMSD	The current guidance in relation to VSP's produced by the Commission is designed to ensure consistent implementation of the definition of AVMSD. As set out we are supportive of this clarity. However, as noted in Q1 of this section, it is already unclear what the situation will be if Facebook's video-sharing platform services (as determined under the Irish implementation of AVMSD) are also regulated services under new German laws that overlap with or are very closely related to AVMSD (or another category of regulated service in another Member State) as the requirements for each legal framework are not harmonised
Ensuring consistency in cross-border application of the rules on the promotion of European works	We are currently not affected by any rules relating to the promotion of European works so cannot comment on whether the current system ensures that the rules are consistently applied
Facilitating coordination in the area of disinformation	ERGA played a role in assessing progress on the Code and we welcomed the close cooperation in this space. However, this exercise has shown that ERGA had a challenge to conduct this assessment on the EU rather than national level.
Other areas of cooperation	

13 **Other areas of cooperation - (please, indicate which ones)**
3000 character(s) maximum

For AVMSD, it would be helpful to have cooperation on:

(1) The remit of content "may impair their physical, mental or moral development" and the risks of subjective interpretation. In particular, certain content may have different meanings in different cultures, so may be inappropriate in one MS but not another; content may be perceived by some as raising awareness but to others as introducing harm (for example, content about tobacco could be introducing the product or raising awareness); and many subjects "may impair... physical, mental or moral development". For example, baking videos featuring recipes high in fat and sugar could be interpreted as harming a minor's physical development and then affect their mental health.

(2) Where appropriate measures may involve the implementation of systems, when such systems are certainly needed as an appropriate measure and when such systems may not be necessary practically to ensure compliance (for example, by reference to the types of services or content that will need such systems).

14 **Are there other points you would like to raise?**
3000 character(s) maximum

Independent Audit
We are looking at opening up our content moderation systems for external audit. We're reaching out to key stakeholders spanning government regulators, civil society, and the advertising industry to help us develop our approach.

Currently, we are preparing an audit of the harmful content metrics we provide in our Community Standards Enforcement Report (CSER). This detailed report shows how we are doing at removing content that violates our Community Standards. The audit, which will be done by an independent auditor, will show that "we're not grading our own homework". We want to give people confidence that the numbers we are reporting around harmful content are accurate. This builds on the work of the Data Transparency Advisory Group (DTAG), who assessed Facebook's methods of measuring and reporting on its Community Standards enforcement policies. In DTAG's final report published last May, it was noted that Facebook's approach and methodology were sound and reasonable.

We will also evaluate our partner and content monetization policies and the brand safety controls we make available to advertisers. This audit, run by the Media Rating Council (MRC), will include (but not be limited to):

- An evaluation of the development and enforcement of our Partner Monetization Policies

- An evaluation of the development and enforcement of our Content Monetization Policies and how these policies enforce the 4A's/GARM Brand Suitability Framework, and comply with MRC's Standards for Brand Safety
- An assessment of our ability to apply brand safety controls to ads shown within publisher content such as in-stream, Instant Articles or Audience Network
- A determination of the accuracy of our available reporting in these areas

More information about Facebook's response:

Aura Salla, Managing Director EU Affairs
aurasalla@fb.com