This document has not been adopted or endorsed by the European Commission. Any possible measures indicated in this paper are the preliminary elements being considered by the Commission services, they do not preclude the measures to be finally considered in the Impact Assessment and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the entity to which it is addressed for discussions and for the preparation of the Impact assessment and may contain confidential and/or privileged material.

IMPACT ASSESSMENT ON ILLEGAL CONTENT ONLINE
STAKEHOLDER CONSULTATION:
INTERNET COMPANIES

Introduction:

In the context of the ongoing work on the Impact Assessment on Illegal Content Online, the Commission would like to get your views on a number of issues set out below. These views will complement the Open Public Consultation (OPC, available here), as well as the data collection exercise based on the table of indicators.

The Commission started work on an impact assessment outlining potential problems, objectives and options in the attached Inception Impact Assessment (IIA). As part of the options to be considered, the Commission will analyse the current situation (baseline scenario) as well as actions to reinforce the voluntary measures as well as possible sector-specific legislation (including in particular on terrorism content online) as well as horizontal legislation applicable to all types of illegal content.

The measures presented in the Inception Impact Assessment[1] are initial ideas, and additional actions and options could be considered. The actions to be undertaken would be mainly addressed to online platforms, but could also require further action by Member States.

In addition to the requests for factual data as part of the reporting exercise within the EU Internet Forum and the possibility to contribute to the Open Public Consultation that closes on 25th June, we would like to offer you the possibility of providing further input to the Impact Assessment by replying to **the questions below and provide any additional considerations in writing by 15th of July.** We are also available on the week of 18-22 June to hold a meeting or videoconference, at a time to be arranged, in order to discuss your input, clarify any questions you may have and discuss additional elements which you consider should be taken into account.

[1] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1183598_en

Questions

1. What are the main risks or concerns for your company as regards terrorist content online which could be hosted in your platform? Please indicate your agreement with the following statements, with a short justification to the extent possible.

Statement	Impact	Justification
Such content has a negative impact on our users	☐ Very negative ☑ Negative ☐ No impact ☐ I don't know	SC is a platform primarily for communicating with close friends. Harmful content would have a negative impact on those interactions
Such content damages the reputational image of the company	☐ Very negatively ☑ Negatively ☐ No impact ☐ I don't know	As above
Such content impacts on the company's business model (e.g. risks of losing advertising or users switching to other platforms)	☐ Very negatively ☑ Negatively ☐ No impact ☐ I don't know	As above
Such content undermines the trust by users when using the Internet	☐ To a large extent ☐ To some extent ☑ To a limited extent ☐ Does not undermine trust ☐ I don't know	Most Intenet users have similar expectations online and offline when it comes to content. Harmful content occurs in both environments
Risks of litigation by hosting such content	☐ Is a serious concern ☐ Is a concern ☑ Is not a concern	We have in place robust Trust & Safety and Law Enforcement Operations capabilities
Risks of diverging legislation in different countries to address such content posing excessive regulatory burden on companies	☑ Is a serious concern ☐ Is a concern ☐ Is not a concern	For smaller companies, it is not possible to comply with 28 different sets of rules. For larger companies, divergence can be used as a tool for competitive advantage
Other; please elaborate:		

2. What measures could be developed to **reinforce the voluntary approach** (e.g. a Memorandum of Understanding or a Code of Conduct between the EU and the industry including specific commitments building upon the Recommendation[2])?

An EU-wide Code of Conduct could be useful - and practical - if Member States agreed not to subsequently issue their own national Codes. What we see with some other content-related EU Codes is that Member States use them as a baseline and create additional, sometimes, contradictory burdens locally. For smaller companies, this creates compliance difficulties and diverts revenue generating resources to compliance tasks, which provide no additional public safety or policy gain. The largest companies can absorb these unnecessary costs without difficulty, particularly if it contrives to cement their already dominant market position. MoUs are generally too general to be of any practical use, beyond political symbolism.

[2] https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

3. Which actions could be taken to **support small companies** and start-ups in tackling terrorist content online effectively? Should these be taken by larger companies, public authorities or both?

1. All necessary steps should be agreed at EU level and apply uniformly across the 28 Member States. Member States should explicitly agree not to adjust EU agreed steps locally.
2. Incentives should be provided to smaller companies to engage in best practice when it comes to all forms of illegal content. For example, lead in times for compliance. Or flexibility of approach in solving the issues.
3. Take down times and automation of process to deal with illegal content should be proportionate to the size and scope of the problem on any particular platform. The largest platforms tend to have the highest volumes and thus the largest problems.
4. Any technical solutions developed by large companies should always be cheap/easy to apply and shared royalty free.

4. What are your views on **regulating at EU level in the following areas** and how would you qualify the **impact on your business (positive or negative)**? Please provide a short justification of your assessment.

Definition of terrorist content	This could be helpful, if 1. all member states adhered strictly to the definition; 2. it was simple and unambiguous; 3. no derogations were created at drafting or later
Requirements regarding the companies' terms of service	The Commission should not be prescribing commercial terms of service, since it is a competitive element of any commercial offering. Broad guidelines for best practice could be helpful, however
General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)	There is already a substantial body of EU and Member State law and regulation relating to how to deal with all forms of illegal content. What is required is help interpreting and applying those rules. What is not required is the creation of new, issue specific rules (for terrorism or any other kind of illegal content), creating confusion and potential conflict with existing legal instruments.
Specific requirements in terms of action upon referral (including time limit of one hour)	Any requirements would need to be sufficiently flexible to accommodate varying volumes of content, audience size, company size, etc. The demand for identical responses from companies with different product offerings and at different stages of economic development would create business imbalances and skew the market irrevocably in favour of the largest, most profitable companies
More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)	Conflicts with existing legal and regulatory instruments should be resolved before any new obligations are created. There also needs to be a distinction between proactive detection in public fora and private communications. This is not well articulated in the current discussion. Proactive scanning of private communications runs counter to historical confidentiality of communications rules and European values. The economic impact on smaller and loss-making companies would be high, were such obligations introduced indiscriminately
Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms	Requiring companies to cooperate is disproportionate and risks cartel-like situations. Already, the largest companies are voluntarily developing technical solutions they provide on a royalty free basis to smaller companies to implement. At one level, this is to be welcomed. At another level, creating any kind dependence on the largest 3 or 4 companies risks ossifying the market, with smaller companies unable to compete unless they cooperate with their biggest competitors.
Sanctions in case of non-compliance	Existing laws and regulations concerning illegal content already provide for sanctions to be applied for non-compliance. Improved application and enforcement of existing rules is clearly simpler (preferable for smaller companies)
Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material	Cooperation with law enforcement beyond formal enquiries should be encouraged. It is in everybody's interests to increase exchanges of information, technological developments, operating methods, education and so on. The fora the EU Commission and other EU bodies provide are useful for industry and create a win-win for all stakeholders.
Clarify that companies	Safe harbours for regulatory compliance are in principle an important safeguard for companies of all sizes and should be encouraged as a matter of regulatory

engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)	good practice. We remain concerned at the unintended consequences of proactive measures (see above). Explicit safe harbours accompanying reasonable measures would have a positive impact on business in terms of legal predictability
Requirement to Member States to increase referral capabilities, quality criteria for referrals and for referral entities in Member States to provide relevant support to companies in case of doubt about qualification as terrorist content (e.g. through points of contact)	Many Member States need to increase their referral capabilities in terms of resource allocation and skills; only a handful operate at a qualitatively high level. We would encourage best practice sharing among Member States, with a view to standardisation of approach across the EU. The European Commission should drive this process to ensure alignment across EU. If this were achieved, the impact on smaller businesses would be positive. The alternative, which is increasingly to farm out wholesale the responsibility to the private sector, raises serious questions about the role of the state in society and the state's duty to protect its citizens as well as uphold their collective beliefs and values
Nomination of point of contact within Companies	We support the nomination of a single Point of Contact within a company. It should be left to the company to decide whether that is an individual or a department
Reporting obligations for companies[3]	We support he introduction of a basic set of annual reporting data, while acknowledging that smaller companies may only report a sub-set of the data, or through a different business model, only generate some data sets
Transparency requirements for companies vis a vis their users[4]	As a matter of good practice, companies should inform their users of how their data is being processed, stored and accessed, including by law enforcement agencies. A comprehensive privacy policy, with related information, for example in a privacy centre, is a good way to achieve this
Compulsory safeguards, such as the ones in the general chapter of the Recommendation	The safeguards foreseen in Arts 19 and 20 of the Recommendation would place a heavy burden on resource-poor smaller and start up companies and negatively impact their ability to scale. The safeguards should only be compulsory for companies of a certain profitability/scale/volume of illegal content. In other cases, the decision on what is illegal should be taken by a public authority or a public authority backed trusted flagger
The establishment of an external audit/monitoring mechanism for assessing compliance of companies.	It is important that the identification of illegal content is not privatised by stealth. The detection, remediation and prevention of criminal activity is one of the key functions of the state. What is appropriate to see, what should be censored or removed and who should be held responsible, is the preserve of the courts, supported by law enforcement and other agencies of state

[3] See point 41 of the Recommendation.

[4] See points 16 and 17 of the Recommendation.