

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.

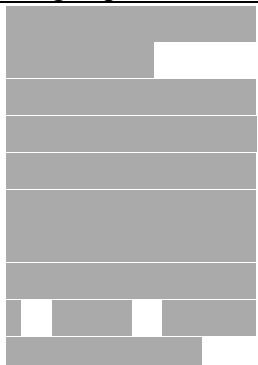
The measures presented in the Inception Impact Assessment¹ are initial ideas, and additional actions and options could be considered. The actions to be undertaken would be mainly addressed to online platforms, but could also require further action by Member States.

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 June**. 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	<input type="checkbox"/> Very negative <input checked="" type="checkbox"/> Negative <input type="checkbox"/> No impact <input type="checkbox"/> I don't know	The content is objectionable to nearly all users.
Such content damages the reputational image of the company	<input type="checkbox"/> Very negatively <input checked="" type="checkbox"/> Negatively <input type="checkbox"/> No impact <input type="checkbox"/> I don't know	Mega and its users don't want to be associated with illegal content.
Such content impacts on the company's business model (e.g. risks of losing advertising or users switching to other platforms)	<input type="checkbox"/> Very negatively <input checked="" type="checkbox"/> Negatively <input type="checkbox"/> No impact <input type="checkbox"/> I don't know	Payment processors may close their facility if illegal content is available
Such content undermines the trust by users when using the Internet	<input type="checkbox"/> To a large extent <input type="checkbox"/> To some extent <input type="checkbox"/> To a limited extent <input type="checkbox"/> Does not undermine trust <input checked="" type="checkbox"/> I don't know	
Risks of litigation by hosting such content	<input type="checkbox"/> Is a serious concern <input type="checkbox"/> Is a concern <input checked="" type="checkbox"/> Is not a concern	Our strict and efficient takedown of illegal content minimises and litigation risk.
Risks of diverging legislation in different countries to address such content posing excessive regulatory burden on companies	<input type="checkbox"/> Is a serious concern <input checked="" type="checkbox"/> Is a concern <input type="checkbox"/> Is not a concern	It is burdensome to find out and implement possible different requirements for the 245 countries / territories in which Mega operates
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 Recommendation²)?

It would be an incentive for voluntary compliance if EU certifies that a platform is performing acceptable takedown etc. activities, AND Visa/MasterCard & payment processors use that certification to exempt platforms from being subject to adverse compliance actions regarding illegal content being ‘hosted’.

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?

There are already forums such as Tech Against Terrorism and Global Internet Forum to Counter Terrorism but they need to be communicated more widely.

A code of practice might be helpful.

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	Not needed for Mega – we act on any type of “Violent Extremism”
Requirements regarding the companies’ terms of service	Likely to be unduly complicated. EU should specify outcomes and let platforms implement actions in the most appropriate manner for their circumstances.
General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)	<p>‘Do not host...’ is an impossible concept as content is uploaded before a platform is aware of it. The only possible objectives are:</p> <ol style="list-style-type: none"> 1. Action: Terrorist content is taken down [and communicated to authorities?] as quickly as possible; and 2. Reporting: [Monthly or Quarterly] Takedown statistics are provided to XX. 3. Communication: The non-acceptance of terrorist content is communicated to users / the public.
Specific requirements in terms of action upon referral (including time limit of one	Mega processes most notifications within a few minutes, but some may take 2 - 4 hours if they arrive after the northern hemisphere shift has finished and

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

hour)	before the southern hemisphere shift has started & v.v. Thus an absolute limit of one hour is not appropriate. It would be acceptable as a target with achievement statistics reported.
More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)	<p>Automatic detection is not a practical/feasible process.</p> <ol style="list-style-type: none"> 1. YouTube has sophisticated systems to screen content that only work to a limited degree even though YouTube/Google has immense resources available, far exceeding what most companies have. 2. YouTube is only dealing with simple unencrypted audiovisual content. Encryption, whether Mega's user-controlled encryption or something as simple as converting content to a zip or rar file, makes automated screening impossible, ineffective and pointless. 3. Most platforms are open to many file types that would not be handled by the YouTube-type screening. 4. The hash databases for pictures and videos have very limited effectiveness because users change the files sufficiently to create new versions that don't match existing hashes. <p>It should only be considered for services that curate user-generated content.</p>
Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms	It isn't possible to avoid dissemination , but it would be useful to share contact details to report content/pages/groups to other platforms.
Sanctions in case of non-compliance	This would be an extreme measure and probably could only be applied to local platforms, so the worst actors in other jurisdictions wouldn't be affected. This should only be considered after reviewing individual platforms and establishing whether there is a problem or not.
Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material	Clarification on exemptions from GDPR would be useful. E.g. GDPR requires users to be notified if their personal data is provided to another party (Art. 15.1c), but Commission Recommendation of 1.3.2018 on <i>Measures To Effectively Tackle Illegal Content Online</i> paragraph 10 notes that content providers do not deserve the usual notices regarding takedown of illegal content. This exemption should be extended to allow sharing personal data with competent authorities (consistent with Art. 23.1a-d), and to acting on referrals from parties other than a competent authority. (Note that Mega receives a large proportion of notifications from private individuals).

Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)	It is very important to recognise platforms with good compliance and reporting regimes.
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)	Mega doesn't have any concerns with the existing reporting activities.
Nomination of point of contact within Companies	Are there any platforms that don't have contact details?
Reporting obligations for companies ³	The recent requests for statistics have created significant work for Mega but we accept that obligation without complaint. However reporting should not be expanded significantly as it could become too burdensome for small companies.
Transparency requirements for companies vis a vis their users ⁴	Mega already has significant disclosure through its Privacy and Takedown policies and annual Transparency Report. Any regulations should be simple, and only considered after reviewing individual platforms and establishing whether there is a problem or not
Compulsory safeguards, such as the ones in the general chapter of the Recommendation	Mega doesn't use automated means so it doesn't have an opinion on the need for safeguards. However generally we act on all reported terrorist content without any preview, as if it is incorrectly taken down the user can appeal and reinstatement can then be considered. An obligation to review reported content should NOT be imposed.
The establishment of an external audit/monitoring mechanism for assessing compliance of companies.	This should only be imposed on individual companies if/when a problem is identified with particular platforms.

³ See point 41 of the Recommendation.

⁴ See points 16 and 17 of the Recommendation.