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	Content which promotes or incites terrorism has no place on our platform. It violates our acceptable use policy and we take steps to remove it and prevent it from reappearing. Dropbox does not provide a mechanism to facilitate discovery of users' content or to create social links between users. The volume of referrals we receive for alleged terrorist content is extremely low. We do not believe, therefore, that terror content has a significant impact on our users. That said, we recognize the negative impact of this content on Internet users generally and on society at large.
Such content damages the reputational image of the company	☐ Very negatively ☐ Negatively ☐ No impact ☒ I don't know	We have not evaluated the reputational impact of such content on our business. Given the low volumes referenced in question 1 we would not expect it to be a significant factor at present, however, we are not complacent about the potential for reputational impact. The trust of our users is of the utmost importance to our business. We see our work to remove harmful or illegal content that is referred to us as very important to maintaining that trust. We believe it is critical to do this in a manner that is also protective of our users' privacy and freedom of expression.
Such content impacts on the company's business model (e.g. risks of losing advertising or users switching	☐ Very negatively ☐ Negatively ☐ No impact ☒ I don't know	Our business model is not based on advertising, we do not promote or monetise public distribution of user generated content, hence our platform is not optimised for such content. Our business model is purely subscription based. Given the low volumes referenced in question 1 we think this is unlikely to be a significant factor in switching to other platforms.

to other platforms)		
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	We have not evaluated the impact of such content on trust in the Internet. We do believe, however, that the way potentially harmful content shared on the Internet is dealt with is relevant to user trust. Removal needs to be effective and timely, but also subject to appropriate review that factors in relevant context and does not create perverse incentives for over-removal or unduly interfere with freedom of expression.
Risks of litigation by hosting such content	☐ Is a serious concern ☐ Is a concern ☐ Is not a concern	Risk of litigation is not currently a significant concern for our platform. If changes were made to the current liability regime for service providers as set out in the eCommerce Directive, this may have implications for litigation. However, a much more significant concern would be the impact that this could have on providers' approach to content takedowns, the potential for over-removal and the implications for freedom of expression and user privacy.
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	Diverging legislation in this area would be unhelpful. It would potentially create additional resource requirements which would be burdensome for smaller companies and companies that have small volumes of referrals. Additionally, it may put companies in conflict of law situations. A voluntary approach, encouraged by the Commission, has the potential to allow for consistency for businesses that operate across jurisdictions. At the same time, it avoids a blanket approach that treats all platforms in the same way regardless of business model, nature of services or scale of the company or problem.
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])?

A very important aspect of measures to reinforce the voluntary approach will be to ensure they are fit for purpose for different platforms of different sizes and business models.

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?

Interaction between larger companies that have been at the forefront of the debate on terror content and smaller companies and/or companies with different business models is valuable. Whilst support with automatic detection may be helpful for some platforms or services, it is not always the best tool (see below question on specific measures) and other exchange of information could be valuable. As a platform that does not offer channels for publication or dissemination, cooperation with others offers a potential opportunity to tackle such content at a point when a) the context is known and b) it is being shared widely.

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	The challenge of defining terrorist content is that context is critical. Some material may not be illegal to possess but may be harmful when disseminated. This is especially challenging for platforms that do not offer channels for publication or dissemination as no context is available. Content that may be valid to possess for journalistic or academic purposes may be problematic in other situations. Any definitions of terrorist content must be drafted in a way that does not undermine the rights, freedoms or privacy of users who have legitimate purposes.
Requirements regarding the companies' terms of service	We believe that the Commission's current approach of engaging with companies, in a voluntary capacity, over how they tackle this issue in their terms of service is the most appropriate route. Different business models, different platforms or services and different user experiences mean that a one-size-fits-all approach is not

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

	optimal.
General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)	We believe that it is already well understood and accepted by companies that they have a responsibility to tackle terrorist content. Companies are continually improving their efforts in this area and the work of the Commission has been effective in encouraging this. A general requirement would raise questions in relation to the liability regime as established in the eCommerce Directive which in turn would have serious implications as discussed above.
Specific requirements in terms of action upon referral (including time limit of one hour)	We do not believe a blanket time limit is appropriate. Smaller companies and companies whose business models mean that they have modest volumes of referrals will struggle as a one hour time limit effectively means having multiple reviewers with the appropriate training and language skills available 24/7. This is especially key for platforms that do not have the context to a piece of content (see question above on definitions) as it is even more important in these circumstances to ensure human review of the content. A one hour takedown time may create an incentive to remove content by default without proper review. This would have implications for user privacy and freedom of expression. We believe it is appropriate to work with businesses to consider what requirements are appropriate taking into account the nature and size of their business.
More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)	We do not believe obligations to deploy specific measures would be helpful given the comments above about the differing nature of platforms and services. Automatic detection, for example, has privacy implications for users particularly in relation to material that is not illegal per se and which can be possessed for valid reasons, and particularly for services where the context for that content cannot be understood. A link to a document in a cloud storage service may well provide no clue to the intention of the user; it is only at the point of dissemination via some other means that the context may become clear. Further, such obligations would raise questions in relation to the liability issue referenced above.
Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms	Again we believe that this is best managed by industry on a voluntary basis given the differing nature of platforms and services. However, it is an area which we are currently giving consideration. As mentioned above, as a platform that does not offer channels for publication or dissemination, cooperation with others offers a potential opportunity to tackle such content at a point when a) the context is known and b) it is being shared widely.
Sanctions in case of non-	As discussed above we believe a voluntary approach is

compliance	most appropriate given the differing nature of platforms and services. Sanctions may create perverse incentives to take down content in ways that limit freedom of expression.
Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material	We are not clear what is proposed here.
Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)	We believe that undermining the current liability exemption has serious negative implications as detailed above. We do not believe that the liability exemption should be linked to the introduction of specific measures, given our comments above on specific measures and automatic detection.
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)	We do not feel there is a necessity to place a requirement on member states on these matters. It is helpful, particularly for platforms that do not have context around the content, when referral entities can provide context based on whether and how the content was published or disseminated. However, we feel that voluntary engagement can be effective here.
Nomination of point of contact within Companies	We have dedicated channels for engagement and are currently reviewing this to consider whether we can further enhance our practices here. We do not believe there is a need to mandate a point of contact.
Reporting obligations for companies[3]	We already report on content takedown in response to government requests as part of our transparency reporting. This is reported at country level and includes information on the volumes of requests and whether or not content was removed.
Transparency requirements for companies vis a vis their users[4]	We do not believe this requires regulation. We already provide transparency to users via our acceptable use policy, terms of service and transparency reporting.
Compulsory safeguards, such as the ones in the general chapter of the Recommendation	As discussed above we believe a voluntary approach is most appropriate given the differing nature of platforms and services.
The establishment of an external audit/monitoring mechanism for assessing compliance of companies.	We do not believe this is necessary. We already report on takedowns as detailed above. Further it is always evident to those referring whether referred content has or has not been removed. For organisations with small volumes, additional audit requirements would burden

[3] See point 41 of the Recommendation.

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

	the teams whose efforts are better spent on focusing on content review and takedown.