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	*Microsoft recognises the harm caused by terrorism- and extremism-related content and has taken a strong stance against the availability of this content on its hosted consumer services, as described elsewhere in this response. However, Microsoft's core solutions and services differ significantly from many hosting service providers, whose primary offerings include, e.g., social media platforms or video-sharing / user-generated content ("UGC") sharing platform. Microsoft's hosted consumer services include Xbox Live, which enables users to communicate with each other in a closed group and in the specific context of online video gaming; and OneDrive, which is primarily a private cloud hosting platform). Microsoft thus does not see the volume of terrorist content on its services as other consumer-facing hosting service providers.*
Such content damages the reputational image of the company	☐ Very negatively ☒ Negatively ☐ No impact ☐ I don't know	*See 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	*See 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	*See above. Microsoft recognises that the wide dissemination of terrorist content online could undermine trust in the safety of the Internet in general. That is why Microsoft has taken multiple steps , including via our notice-and-takedown process; the advancement of counter-narratives; the use of technological solutions; the use of technological*

		solutions; a dedicated process for reporting the presence of terrorist content on Microsoft's hosted consumer services to Microsoft by government authorities and others, which process will notify the reporting entity or person as to Microsoft's conclusion on whether terrorist content has been found; close collaboration with other providers; and the sharing of knowledge and best practices across stakeholder groups to prohibit terrorists from exploiting online platforms. *Separately, for Microsoft's Bing search service[2], we have been working with an external partner on a pilot project to show counter narratives (e.g., video testimonials from former terrorist recruits) via Bing search ads.*
Risks of litigation by hosting such content	☐ Is a serious concern ☒ Is a concern ☐ Is not a concern	*The highest risk of litigation arises with respect to the allegedly wrongful removal or disabling of hosted content – for example, litigation brought by users of the service who contest the legal basis on which their content was removed.*
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 across the EU would create significant compliance complexities for hosting service providers. Variations in the requirements within each jurisdiction can create conflicts of law that makes compliance challenging and can also add uncertainty to decision-making that may hamper response times.*
Other; please elaborate:		*Not all content or platforms are alike, and one size does not fit all. Different types of content have different legal and social implications, and different online platforms play different roles in the online ecosystem.*

[2] Our Bing search engine strives to be an unbiased information and action tool, presenting links to relevant information available on the Internet. Like other search engines, Bing generally does not host content itself.

		As a result, the two most critical pivots for our principled approach are: *1) the **nature of the content**, and* *2) the **nature of the service**, its role in the ecosystem and how users access and engage with that content online.* *Currently there is no universally accepted definition of what constitutes "terrorist content". Microsoft defines terrorist content in respect of its own services to mean material posted by or in support of individuals or organizations included on the Consolidated United Nation's Security Council Sanctions List that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups.*

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[3])?

A Memorandum of Understanding between industry and the EU and/or an industry-regulated Code of Conduct are both interesting ideas. We would welcome the opportunity to discuss these options with the Commission in more detail.

There are many industry-led initiatives for tackling terrorist content online (and other illegal content online) that are already in progress, as the Commission is well aware. Just some of the initiatives in which Microsoft is involved include:

- *An alliance between Microsoft and some of the world's largest hosting service providers (including Twitter, Facebook and YouTube) aimed at combatting the dissemination of terrorist content online through knowledge-sharing, technological development and research. The alliance operates under the auspices of the Global Internet Forum to Counter Terrorism ("GIFCT"): https://blogs.microsoft.com/on-the-issues/2017/12/04/facebook-microsoft-twitter-and-youtube-provide-update-on-global-internet-forum-to-counter-terrorism/.*
- *A partnership with the Institute for Strategic Dialogue on a program that enables NGOs to serve advertisements on Bing that provide a counter-narrative in response to searches for thousands of terrorism- and extremism-related search terms.*
- *A paid-for subscription service with a third-party intelligence service that flags to Microsoft on a near real-time basis new terrorist content that has been posted to its OneDrive cloud storage service.*

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

- *Microsoft reviews and removes terrorist content on our hosted consumer services reported to Microsoft by Europol and Member State Internet Referral Units.*

Microsoft encourages the Commission to build on these (and other) initiatives to leverage the substantial investments that have already made in tackling these issues, and also to avoid duplication of efforts.

Any voluntary measures introduced should also be specific to the category of illegal content in question (recognizing, for example, that the approach taken to combatting terrorist content online may need to be different based on the nature and context of the content). Those measures should also take account of the variances between different types of service providers, that reflect the ways they host and distribute content – for example, public-facing social media and video-sharing platforms are often specifically designed to enable public dissemination of content and thus raise qualitatively different risks compared to services intended primarily for private communications, such as cloud storage services and private messaging platforms.

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?

Microsoft, through the GIFCT collaboration (described above), has partnered with the Tech Against Terrorism initiative (https://www.techagainstterrorism.org/) to engage with and provide ongoing support for smaller tech companies – for example, by holding workshops to share best practices for countering terrorist content online and other knowledge-sharing. The Tech Against Terrorism initiative was implemented by the ICT4Peace Foundation under a mandate from the UN's Counter-Terrorism Committee Executive Directorate.

The Commission should support and promote continued cooperation between larger and smaller technology companies in this space. Member State public authorities also have an important role to play, by acting as facilitators between industry players, and by educating smaller companies on the issues and on tools / programs available to promote best practices, such as the GIFCT.

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.

Note to the Commission: We have responded to the statements below on the assumption that the Commission's questions relate only to a possible regulation on combatting online terrorist content. If the Commission is contemplating horizontal legislation that would address all forms of illegal content online, however, we would like an opportunity to revisit these responses. Microsoft encourages the Commission to avoid a "one-size-fits-all" approach to policy-making in this area; as noted above, to be effective, and ensure an appropriate balance of interests,

any proposals in this area (for regulation or otherwise) must take adequate account of the variety of hosting service providers and the fact that different types of illegal content may merit different responses.

Our responses also do not indicate whether the impact of any of the measures below would be "positive" or "negative" on our business. Ultimately, the impact depends on the nature, approach and details of any regulatory proposal. We would require more information in order to be able to meaningfully comment.

Definition of terrorist content	*Currently there is no universally accepted definition of what constitutes "terrorist content". Should the Commission choose to regulate, any regulation should include a clear and harmonised definition of the content it is targeting. The concept of "terrorist content" would also need to be defined in a manner that is consistent with international norms. Microsoft defines terrorist content in respect of its own services to mean material posted by or in support of individuals or organizations included on the Consolidated United Nation's Security Council Sanctions List that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups.*
Requirements regarding the companies' terms of service	*As is the case with other major hosting service providers, Microsoft's terms of use prohibit users from posting terrorist content on our services (the Microsoft Services Agreement contains a Code of Conduct where the prohibition is explicitly stated: https://www.microsoft.com/en-gb/servicesagreement/). Microsoft takes the enforcement of these terms very seriously.* *Any contemplated regulation regarding companies' terms of use should not be prescriptive as to the specific provisions to include in terms. Instead each service provider should be able to set its own terms consistent with nature and purpose of each type of service it offers (e.g. a closed communications or hosting service versus a public-facing video-sharing or social media platform) and the specific challenges it faces with respect to the dissemination of different types of illegal content.*
General requirement for companies to put the	*Regarding the removal of user content from cloud services, it is important to distinguish between: (A)*

necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)	*government laws, order or actions to remove content; and (B) cloud service providers' removal of content in order to maintain the nature and purpose of the service and meet the needs and expectations of users (e.g., through terms of use, code of conduct, or community guidelines for the service).* *In the context of government laws, order or actions to remove content, international human rights laws have long recognized the human right to freedom of expression. It is a key contributor to human dignity and the development of human potential. Of course, any technology, whether the printing press or the cloud, can be misused to disseminate illegal or harmful content. This raises important questions for governments, communities, cloud service providers and other stakeholders, who seek to ensure freedom of expression, and the right to receive and impart information on the global internet while protecting public safety. As societies seek to protect human rights while combating content such as terrorist or extremist content, it is important to recognize that public safety and human rights are complementary values that reinforce each other.* *Governments should adopt clear laws and regulations that are interpreted and administered under the rule of law, including advancement of international human rights laws and norms. This will enable governments to protect freedom of expression and public safety while continuing to support robust exchange of ideas and information to fuel the benefits that technology can bring to societies and economies.* *In particular, governments should consider the following principles:* 1. *<u>Adhere to the rule of law</u>. In regulating online content, governments should fully commit to the rule of law. This means ensuring that laws and regulations and their enforcement are transparent and respect international human rights laws and norms. Governments should be open and engage their citizenry in public debate on the enactment of laws and regulations regarding restriction of online content. Citizens should determine how such laws and regulations will be enforced. Rule of law requires that enforcement orders and decisions be subject to independent judicial approval and*

	review, with meaningful and trusted opportunity for companies and individuals to appeal judicial approvals or decisions. Adherence to rule of law will serve best to ensure that the benefits of cloud computing lead to human development and economic advancement. 2. *<u>Adopt a principled approach to online content regulation and protect freedom of expression</u>. One of the fundamental roles and responsibilities of governments is to protect public safety. This sometimes requires the regulation of online content. Any governmental restriction on freedom of expression should respect the norms established by international law: legality, necessity and proportionality. Restrictions should be duly enacted by law, should be the least restrictive means possible and should be proportionate to the legitimate objective. Governments should ensure that laws are strictly limited to the protection of public safety, and do not prevent broad sharing of ideas — even ideas that are unpopular.* 3. *<u>When governments demand that online service companies remove content, they should do so transparently</u>. These demands should be made pursuant to laws and regulations that clearly define what constitutes illegal content and the types of services that must remove it. Laws and regulations should require that legal orders for the removal of illegal content be specific, narrowly tailored and sufficiently detailed to enable companies to identify precisely which content must be taken down. Such laws and legal orders should not require companies (directly, or indirectly through intermediary liability or other pressures) to proactively monitor content or make independent determinations of illegality. Laws and regulations should not restrict companies from informing the public about removal demands from governmental authorities.* 4. *<u>Respect national sovereignty through international cooperation</u>. Given the transnational nature of the global internet, demands to remove content will often affect other jurisdictions. Unilateral demands or actions risk violation of other countries'*

	sovereignty, conflict of laws among nations, and potential interference with the exercise of fundamental rights. Governments should focus on strengthening international cooperation and adhering to international norms in considering content regulation on the global internet. Where existing rules or processes for cross-border cooperation are outdated or cumbersome, governments should work together to update them so they keep up with new technologies, are adequate to address new challenges and protect human rights. Self-help is never the best option. 5. *<u>Noninterference with technology companies' terms of use</u>. As noted in the first paragraph of our response to this question, cloud services that permit end users to post content for viewing by others usually include terms of use (aka terms of service). These terms of use are designed to advance the service provider's legitimate business purposes for the service in question, including generation of experiences appropriate to the nature of the service and the user communities they serve. Companies generally provide processes for users or others to report content that may violate the terms of use, and have procedures for review and removal of content that violates applicable terms of use. Governments should not pressure companies to change their terms of use or interfere with the way they are enforced.* *If the Commission were to introduce regulation on tackling terrorist content online, a broad and general obligation requiring covered entities to implement effective measures to combat terrorist content would be preferable to prescriptive requirements as to the type of measures to be deployed and the form that they should take. Hosting service providers should be able to continue using measures that are already having a positive effect on reducing instances of terrorist content and should have flexibility with respect to future technology deployed; any other approach would be ineffective and risks chilling innovation in this area.* *Importantly too, any prospective regulation should make it clear that where hosting service providers discover illegal content through the use of voluntary, proactive measures they remain within scope of Article*

	14 of the E-Commerce Directive, on the condition that they have exercised their duty of care.
Specific requirements in terms of action upon referral (including time limit of one hour)	*As noted immediately above, if the Commission regulates, it should set general parameters for hosting service providers, including with respect to taking action upon referral (such as confirming receipt of a referral from a competent authority: for example, Microsoft already has a process in place whereby a person or organisation that reports suspected terrorist content on Microsoft's hosted consumer services receives a return email indicating whether the content reported was, in fact, terrorist content and, if so, the time at which action was taken against both the content and the offending account).* *Requiring services to remove or disable access to all terrorist content within one hour from the time they receive a referral is unworkable in practice. Service providers need time to assess the nature of the content (and potentially seek clarification from the referring party). A one-hour deadline is more likely to result in erroneous decisions and the over-removal of content.* *It would be more proportionate for any regulation to impose a requirement on platforms to remove suspected terrorist content "expeditiously" and in a time frame that is reasonable.* *In cases of imminent harm, Microsoft has a process in place for reporting activity to law enforcement and relevant authorities where Microsoft has a reasonable belief that a person is at risk of imminent bodily harm, such as suicide, threats of physical violence, imminent (or ongoing) unlawful physical contact with a child and active terrorist or extremist threats. While Microsoft does not generally report customer content or behavior to law enforcement absent appropriate legal process, exigent circumstances such as a potential life and death situations merit an exception to our general approach. This is a limited exception, as identified by certain, clearly defined parameters.*
More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)	*See our response to the third statement.*
Specific requirements to cooperate with other hosting	*Microsoft is already cooperating closely with other hosting service providers, through the GIFCT, among*

service providers to avoid the dissemination across platforms	*other initiatives. GIFCT members work together to combat the dissemination of terrorist content across different platforms via tools such as the Shared Industry Hash Database, which enables the detection of known terrorist imagery using "hash-matching" technology.* *In addition, Microsoft is currently working with and refining a process with Twitter whereby Microsoft receives from Twitter a list of URLs of known terrorist imagery on Microsoft services. The program is still in beta testing, but with refinements shows promise.* *Any contemplated regulation requiring cooperation among hosting service providers are more likely to cause confusion and stifle the progress and effective development of existing initiatives.*
Sanctions in case of non-compliance	*Sanctions should be reserved for egregious offenders, not for services making good faith efforts to combat terrorist content online through the use of notice-and-takedown procedures, the implementation of automated technologies and collaboration with multiple stakeholders.*
Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material	*Cooperation between law enforcement authorities and hosting service providers is essential to the success of any counter-terrorism initiative. Law enforcement authorities provide the necessary expertise in determining the illegality of content. A reliable channel of communication between the relevant authorities and service providers is also important for keeping service providers informed of when actions taken in respect of terrorist content may impact the prevention, investigation, detection or prosecution of a criminal offence.* *Microsoft already cooperates closely with Europol and EU Member State Internet Referral Units on the detection and identification (and subsequent removal) of terrorist content for take-down. If the Commission decides to regulate in this area, we encourage it to build on existing frameworks to ensure that information can continue to be exchanged efficiently.* *[Please see Protecting both Human Rights and Public Safety in our publication A Cloud for Global Good for our recommendations on law enforcement access to information.]*

Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)	*Any prospective regulation on combatting terrorist content online should include a Good Samaritan clause. This clause should ensure that hosting service providers remain eligible for Article 14 of the E-Commerce Directive (on the condition that they take adequate and proportionate measures to detect and remove access to illegal content when they know or have reason to know of that content on their services). A Good Samaritan clause of this nature will incentivise service providers to act expeditiously in relation to terrorist content on their services.*
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)	*Cooperation between Member States and hosting service providers is an essential component of combatting terrorist content online. Microsoft already promptly review reports of suspected terrorist content from Member State Internet Referral Units.* *Should the Commission decide to regulate in this area, safeguards should be built in that:* • *provide for a liability safe harbour in case the service provider removes content from its platform on the referral of a Member State referral body, which later turns out to have been flagged erroneously.*
Nomination of point of contact within Companies	*Appointment of team responsible for communicating with law enforcement authorities and other trusted flaggers on the removal of terrorist content could be helpful for coordination.*
Reporting obligations for companies[4]	*Microsoft understands from the Recommendation that the obligation to report to the Commission would fall on Member States; hosting service providers, in turn, would be expected to report to Member States on the number of referrals received from Member States and the decisions taken with respect to those referrals. In principle, Microsoft has no objections to reporting to Member States, assuming requirements as to the form or content of the reports are kept broad and flexible so that service providers of all sizes are able to meet this obligation.*

[4] See point 41 of the Recommendation.

Transparency requirements for companies vis a vis their users[5]	*Microsoft is committed to transparency regarding the removal of content from its services and already provides biannual, publicly-available reports on content removal requests – including requests from governments regarding claims of violation of local laws or Microsoft's terms of use (the latest report can be found here: https://www.microsoft.com/en-us/about/corporate-responsibility/crrr/).*
Compulsory safeguards, such as the ones in the general chapter of the Recommendation	*Microsoft is concerned, and recognises the importance of having robust safeguards in place, where hosting service providers are being asked to make decisions as to the legality of content. Microsoft is also acutely aware that the use of automated filtering technologies, for example, can pose risks to consumers' fundamental rights, including rights to protection of personal data, freedom of expression and the freedom to impart information.* *As it stands, the Recommendation does not provide much guidance on safeguards because the relevant paragraphs are drafted in a broad manner (e.g. requiring hosting service providers to institute "effective and appropriate safeguards" and act in a "diligent and proportionate manner" in respect of content that they store and remove). Moreover, the Recommendation requires hosting service providers to act in a way that does not violate users' fundamental rights, but does not articulate what this means in practice in light of the obligations on service providers to detect, identify and (where appropriate) remove user content. We encourage the Commission to provide more clarity on the safeguards and corresponding expectations on hosting service providers. In particular, hosting service providers need assurances that their efforts to tackle online terrorist content will not breach competing obligations, for example under data protection law (including with respect to the GDPR and the prospective E-Privacy Regulation)*
The establishment of an external audit/monitoring mechanism for assessing compliance of companies.	*Auditing / monitoring of compliance by hosting service providers should be secondary to implementing a mechanism that ensures service providers understand their obligations, have access to the necessary tools to comply, can clearly, consistently and objectively determine when content is in fact illegal and must be*

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

	disabled / removed, and have appropriate guidance on how to respond in the face of counter-notices. *If the Commission were to establish an external monitoring mechanism, it should be light-touch, and the decision to submit to an audit should be voluntary.*