AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Fighting Online Terrorist Content

Designing constructive and workable solutions

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2017, directly supports more than 4.7 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive Summary

Members of the American Chamber of Commerce to the European Union (AmCham EU) are fully committed to combating online terrorism as the threat posed to our democratic societies is immense. This position paper includes main recommendations on the proposed regulation on preventing the dissemination of terrorist content online to design constructive and workable solutions, including through a targeted approach, to address this common threat:

- The definition of hosting service providers in the current text is unclear and must explicitly state what kind of hosting service providers and content require proactive measures. The scope should refer to services that enable users to make the content available to the general public;

- The procedure for content removal needs to be consistent and proportionate in order to function effectively. Co-legislators should review the 1-hour deadline for removal and introduce flexibility in recognition that there could be technical or resources restraints;

- There is a need for legal certainty around what the proactive measures should entail, now that they are subject to a binding legislation and possible sanctions. Clear guidelines from the European Commission could help this process;

- Throughout the Regulation, it should be made explicit that proactive measures and transparency requirements are only necessary for hosting service providers that have been exposed to terrorist content;

- The current scale of legal and financial sanctions - combined with vague notions in the proposal - could encourage overzealous takedown by hosting service providers which could undermine EU citizens' freedom of speech;

- The relationship between service providers and the competent authority should be streamlined to a single point of contact.

Introduction

Technological developments - in particular the widespread use of the internet as a tool to disseminate ideas and promote values globally - are essential to promote economic growth, and deliver benefits for society across healthcare, culture and education, to name a few. However, the increasing popularity of online platforms and social media in recent years has also been accompanied by an increase in criminal behaviour, whereby the open internet is misused for illegal activities including for dissemination of terrorist content.

One of the EU's responses to terrorist attacks striking several Member States has been to adopt the Terrorism directive in 2017, which contains language on removing content that 'provokes' terrorist acts. However, the Directive made no reference to other tools except to ensure cooperation between the EU and third countries for 'the removal of online content constituting a public provocation to commit a terrorist offence from servers within their territory.'

To address the increasingly digital nature of criminal activity, the European Commission published a Communication and Recommendation on tackling illegal content, in September 2017 and March 2018 respectively, setting out principles and guidance for hosting service providers to remove illegal content posted on their interfaces. Many of these recommendations form the basis for the Regulation on preventing the dissemination of terrorist content online published on 12 September 2018 (hereafter 'the Regulation'). The Regulation aims at reducing the possibilities for criminals to abuse websites by posting publicly available content which incites terrorism.

AmCham EU members are fully committed to combating online terrorism and this position paper includes recommendations to address this common threat.

A clear scope and set of workable definitions

Definition of Hosting Service Providers

In order for the Regulation to be effective, protect fundamental rights and work in practice, the definitions and scope need to be clarified. Our members welcome the effort to address the serious problem of terrorist content online, and therefore, the process for doing so must avoid legally ambiguous terms in order to be as effective as possible and circumvent unintended consequences.

The proposed definition of hosting service providers risks capturing a significantly broader group of providers (article 2.1, Recital 10). The wording 'making available to third parties' is problematic as it is not clear what types of providers this encompasses and could entail that business-to-business cloud providers, or any cloud-based service that allows users to collaborate with other pre-defined and limited private set of users, could be caught by the proposal. This would impact Software as a Service (Saas) and Infrastructure as a Service (Iaas) businesses, despite the content they host not being accessible to the public and these services not being suited to disseminate or communicate information to the broader public. **Instead, the scope should refer to services that enable users to make the content available to the general public.** Recital 10 as amended in the Council's general approach has the merit to clarify impact on certain service providers. However, the notion of 'third parties, understood as any third user' remains vague.

Definition of Terrorist Content

We welcome the **clear alignment of definitions in this Regulation and the provisions of the 2017 Terrorism Directive** in the Council's general approach (which links the definition in article 2 paragraph 5 to article 3(1) (a) to (i) of the Directive 2017/541). An unclear definition of the type of content from hosting service providers, combined with high penalties, risks leading to over-removal which would undermine the freedom of the internet and rights of users. The definition as included in the Commission's proposal also fails to clarify the roles and responsibilities of judicial authorities and private hosting service providers in determining what constitutes terrorist content. It is important that hosting service providers are not rendered arbiters of truth through

assigning a decision as to the illegality of a piece of content. This is the responsibility of legal authorities and the courts.

A consistent and proportionate system for removal

Removal orders

The Regulation puts the onus on hosting service providers to remove content flagged as terrorist within one hour from receipt of the removal order (article 4.2), combined with a heavy sanction in case of systemic failure (article 18(4)). It is virtually impossible for any hosting service provider, especially smaller ones, to take down content within 1 hour. There may be cases where a service will be able to meet the deadline, however this will often depend on the circumstances and nature of the order, the size of the provider as well as resources or technical restraints. We therefore recommend that co-legislators **review and introduce more flexibility whilst at the same time ensuring a swift take down of notified content**. This could be done by replacing the 1-hour deadline with '**expeditiously**' in article 4 (2), whilst clarifying in Recital 13 that a hosting service provider should undertake best efforts to remove or disable access within one 1-hour otherwise 'expeditiously' if there are technical or resources constraints.

Furthermore, for the purpose of legal certainty, the language used throughout the Regulation should be consistent. In the Commission's proposal it ranges from 'without undue delay' under article 4(6) to 'expeditiously' in article 5(6), and 'as a matter of priority' in article 5(5). We see room for confusion in all these uses and call on co-legislators to **align the different terms with the commonly accepted wording of the GDPR, namely 'without undue delay'.** In this regard, we welcome the amendment introduced by the Council's general approach on article 5(6), which should also be reflected in article 5(5).

Proactive measures

In recognition of the proliferation of certain egregious categories of illegal content online, such as child exploitation material and terrorist content, additional steps have been taken by many online actors to ensure that this content is removed at the earliest possible stage. For example, hashing databases shared among industry players which allow them to share and 'hash' violating images so as to prevent their upload on social networks and other sites. There is shared acknowledgement that even more can be done in order to combat harmful illegal content online.

There is a need for legal certainty around what the proactive measures should entail, now that they are subject to a binding legislation and possible sanctions. **Only hosting service providers which have been 'exposed to terrorist content' should be required to implement proactive measures** (as amended by the Council's general approach, article 6 paragraph 1 (proactive measures)). Furthermore, we encourage the Commission to produce **clear guidelines to help this process, and the co-legislators to clarify the interaction of this procedure with the existing framework, in particular the e-Commerce Directive.**[1]

The Regulation also needs to clarify who the competent authority is and their specialism in advising hosting service providers about the effectiveness and appropriateness of proactive measures they have introduced (article 6(4)). Finally, we recommend that a time limit of 72-hours is introduced (instead of 'within a reasonable period of time') for the competent authority to respond to a hosting service provider's request to revoke a decision which imposes proactive measures on them (article 6(5)).

Transparency

The transparency requirements of article 8 should only be applicable to hosting service providers that are exposed to terrorist content. Mandatory annual transparency reports do not make sense when the hosting service provider has extremely limited risk of exposure to terrorist content. **Article 8(1)** should read that 'Hosting service providers, **exposed to terrorist content**, shall set out in their terms and conditions their policy to prevent

[1] Articles 14 and 15 of the e-Commerce Directive provide a limited liability regime for online players, under certain conditions

the dissemination of terrorist content'. Furthermore, we welcome the amendment introduced in the Council's general approach in recital 24 and article 8(2).

A proportionate sanctions regime

As provided in article 18(4), 'systematic failure to comply with article 4(2)' - the one-hour removal of terrorist content after a judicial order - would expose the hosting service provider to a fine of 4% of its turnover in the previous year. Whilst we fully understand the need to penalise wrongdoers, we are wary that **the scale of the legal and financial sanctions could encourage overzealous takedowns of content by hosting service providers.**

Furthermore, as mentioned before, due to the current text being unclear as to when proactive measures are required, hosting service providers may interpret their obligations differently compared to the view of law enforcers. This could render them non-compliant and place them at risk of a heavy penalty despite having the best intentions to follow the law.

Competent authorities

The relationship between service providers and the competent authority should be streamlined to a single point of contact. The current proposal foresees a system whereby any competent authority in any Member State would be able to issue a removal order and levy a sanction regardless of where the service provider is legally established. This raises a number of questions regarding jurisdictional competence, but also in practice because service providers would need to put in place an infrastructure to field these requests from all Member States. This would be disproportionately costly for smaller providers without leading to better outcomes. Single points of contact allow for more open and closer relationships which in turn results in better understanding and more efficient and quicker response times.

Conclusion

AmCham EU members stand ready to support tackling the dissemination of terrorist content online. We hope that co-legislators will enhance the Commission's proposal by designing workable and constructive solutions. This requires first and foremost the clarification of legally ambiguous terms. Through a targeted approach we can prevent a sanction regime that risks leading to overzealous takedowns of content by hosting service providers and avoid undermining the widespread use of the internet as a tool to disseminate ideas and promote global values.