GSMA/ETNO position paper on the European Commission's Proposal for a Regulation on preventing the dissemination of terrorist content online

COM(2018) 640 final

I. Executive summary

Over the last years, the European Commission has proposed measures to further increase the fight against illegal content online. The latest proposal of September 2018 aims to prevent the dissemination of terrorist content online. GSMA and ETNO fully endorse the objective of the European Commission to effectively tackle the dissemination of terrorist content online.

At the same time, we are concerned that the draft regulation could have unintended effects, such as affecting telecom providers that in fact do not provide users with the capability to upload and share third party content to large audiences. Some of the services provided by GSMA and ETNO members are currently in the scope, to the extent that they act in the role of hosting service providers by offering cloud storage solutions. Given the broad range of proposed measures and related penalties, we believe that the scope of the initiative should be more carefully targeted to not unduly affect information society services and infrastructure providers that only operate on the edge of the public web. Furthermore, the suggested measures may disproportionately harm European citizens' fundamental rights to information and expression protected by existing EU law.

We would like to propose the following recommendations to make the proposal workable and proportionate:

- As set out in the Explanatory Memorandum, the regulation is meant to have a targeted scope focusing on hosting service providers allowing *"upload of third party content"* and that *"have the ability to reach such a large audience*" (COM(2018) 640 final, p. 1). This is also in line with the Commission's previous initiative on self-regulation by large social media platforms. The targeted approach should be strengthened in the legal text by ensuring that cloud storage services with a predetermined group of users such as corporate intranets, are not covered.
- The proposal needs to better align with the eCommerce Directive (hereafter eCD). The definition "hosting service provider" creates legal uncertainty, as contrary to the eCD it does not include a clear exemption from liability for information society services whose activity is of a mere technical, automatic and passive nature. In addition, as an effective tool to strike the correct balance of rights and obligations in the Internet ecosystem, the judicial oversight and legal certainty of the liability exemption in the eCD should be maintained.
- Sufficient time should be given to the hosting service provider to: undertake the technical activities ensuring the order's completeness; make sure it can be carried out correctly; and

avail of the possibility to appeal the decision. The required response time should be proportionate to the level of risk and exposure to terrorist content of a platform.

- While the proposal calls for a harmonized framework, there is a risk of fragmentation as the definition of "terrorist content" comes from a directive (Article 2).
- There should be a single authority in each Member State for issuing removal orders and referrals, to avoid technical difficulties and potential security risks in transmitting the requested information.
- To remove terrorist content efficiently, the evaluation of content should always fall under judicial review of the Member State in which the provider has its main establishment.
- Finally, the regulation goes beyond what is necessary to ensure the intended purpose. The provisions on duty of care (Article 3) and proactive measures (Article 6), which add to the obligation to remove or disable terrorist content further to a removal order, would represent disproportionate obligations. This could lead to legal uncertainty for hosting providers, especially in combination with the lack of clarity around the definition of hosting service provider.

II. Ensuring a targeted approach and legal certainty

To ensure a proportionate and efficient response to the issue of terrorism content, the Explanatory Memorandum of the regulation proposes a targeted approach focusing on hosting service providers *"that allow the upload of third party content"* and that *"have the ability to reach such a large audience*". However, the definition (recital 10 and Article 2) covers social media platforms, video streaming services as well as file sharing and other cloud services to the extent they make the information available to third parties, and websites where users can make comments or post reviews. This would also include services that do not reach a larger audience. Telecom operators, in their role as cloud service providers, are therefore within scope of the regulation.

Keeping the current definition would pose both technical and legal constraints where cloud storage services are encrypted and/or do not provide the capability to upload and share content with a wide audience. The text should therefore clarify that the proposal does not apply to cloud storage services that are encrypted by the content provider, and cloud storage services that allow the sharing of content in a closed environment.

Definition of terrorist content

It is of utmost importance to ensure legal certainty for hosting providers, starting with a common definition of terrorist content. In principle, a detailed definition firmly applicable across the EU is required to provide such legal certainty. As it stands today, the proposal includes a very vague

definition (Article 2) with several references to Directive (EU) 2017/541, which defines "terrorist offence". However, it is unlikely that Member States, given their national prerogatives for national security would provide a more clear and consistent definition, and hence, the regulation could be interpreted differently leading to different interpretations across the EU with potentially very adverse effects on Europeans' fundamental rights. Therefore, and for the sake of legal certainty for hosting providers, co-legislators and particularly Member States should ensure legal certainty for hosting providers in this regard.

III. Technical and legal constraints to the proposed measures

a) One-hour removal orders

The one-hour limit to respond to a removal order imposes a new obligation on providers. They would need to put in place organisational measures that today are not generally built-in due to technical and judicial procedures and constraints. GSMA and ETNO support that the legality of the removal order is determined through judicial review. More time should be provided to respond to the removal order itself. This is essential to give sufficient time to the hosting service provider to undertake the technical review to ascertain that the order is complete, can be carried out correctly, and possibly appeal the decision. This is necessary also in the context of Article 14 of the eCD, as the reception of a removal order would automatically lead to the provider's potential awareness of hosting illegal content. Not removing the content within one hour would cause the loss of the liability exemption of the eCD.

The required response time should be proportionate to the level of risk and exposure to terrorist content of a platform, since the distribution of terrorist content follows a dynamic pattern as shown in the EC impact study. The most stringent response time should only be imposed on platforms with a high level of risk. Other hosting service providers should respond expeditiously.

b) A Single Competent Authority

Requirements on hosting service providers to consider requests coming from multiple competent authorities, including removal orders issued by a competent authority of another Member State (Article 15 (3)), will imply a considerable increase in compliance costs. It will also pose major technical obstacles and potential security risks, as it will be difficult to transmit the requested terrorism information in a secure manner.

The establishment of a centralized, secure transmission channel would avoid the unintended consequences of the implementation of a cooperation system with multiple authorities involved. Therefore, ETNO and GSMA propose a single authority in each Member State to be the sole receiver and issuer of the corresponding orders and referrals as well as the only requesting interlocutor with the hosting platforms.

c) Referral

Referral orders in the proposed regulation are a complement to removal orders as both aim to remove terrorist content. However, referrals are not subject to judicial review determining their legality, and may be issued by bodies from Member States other than the company's main establishment country. This undermines the subsidiarity principle, as a company could become liable for not removing illegal content based on a referral order coming from either another Member State's authority or a Union body such as Europol.

The evaluation of whether the content constitutes terrorist material should always fall under judicial review of the Member State in which the provider has its main establishment. This is particularly important considering the lack of clarity regarding the definition of terrorist content, which is open to different national interpretations. This is in line with the eCD, which allows Member States to empower their competent authorities to impose obligations on intermediaries where illegal activities are deemed to have occurred. This would protect the principles of both subsidiarity and proportionality.

If the referral to remove content is maintained, its wording should clearly state that the one competent authority in each Member State that issues the referral must evaluate and guarantee in advance the proportionality of the measures it prescribes. Judicial oversight over the referrals by the competent authority, or other responsible authority designated by the latter, is essential to guarantee the fundamental rights at stake. The added benefits of this could potentially be an enhanced cooperation of Member States and Union bodies as seen in the e-Codex model.

IV. Avoiding unintended consequences

In the public consultation on the fight against illegal content leading up to the proposed regulation, GSMA and ETNO expressed support for the Commission to preserve judicial oversight and legal certainty of the liability exemption as provided for in the eCD. It is key to ensure that providers acting expeditiously upon knowledge of illegal content be sure of remaining exempted from liability as a key pillar in the digital ecosystem.

We are therefore concerned that the definition of hosting service providers (Article 2) leaves out such liability exemption, which is key part of the definition in the eCD and fundamental to establishing a fair and workable balance of rights and obligations in the Internet ecosystem. According to Article 14 eCD, providers are exempted from liability as long as they do not have actual knowledge or information of illegal activity and act expeditiously upon becoming aware of it. We acknowledge that the proposed regulation states that any measures taken by the hosting service provider in compliance with the regulation should not make a provider lose the benefit of the liability exemption. However, the proposal also states that in some cases *"this Regulation may exceptionally derogate from this principle under an EU framework"* (COM(2018) 640 final, p. 3).

Therefore, there is a risk of contradiction between the conditions for enjoying the liability exemption in the eCD (Article 14) and the provisions in the proposal at hand.

Changing the liability exemption is especially worrying in view of the broad scope. As stated in Recital 10, the regulation should apply to information society services irrespective of whether their "*activity is of a mere technical, automatic and passive nature*". This requirement would be impractical, as only hosting service providers who have an active role and insight in handling content will be able to properly enforce the proposed measures of the regulation. It is also contrary to CJEU jurisprudence, which has established actual knowledge (as opposed to generalised knowledge) as a fundamental factor in determining the liability of online Intermediaries (Case C-324/09 *L'Oreal v eBay*). Thus, it is crucial to amend the wording of the regulation to ensure a targeted scope, as described in part II of this paper. The eCD is a sound instrument providing legal certainty for operators and protecting the freedom of information and expression and the freedom to do business. This cornerstone of the EU's regulatory framework should be kept intact.

a) Duty of care and proactive measures

The provisions on duty of care (Article 3) and in particular, proactive measures (Article 6) are technically challenging and potentially unworkable. Such measures would represent a disproportionate obligation on hosting providers who will have to monitor the web to detect the (not clearly defined) terrorist content and to prevent its dissemination, without an order from a competent authority.

ETNO and GSMA believe that, to the extent private companies are encouraged by lawmakers to put in place self-regulatory measures on the use of automated tools, including development and sharing of such tools in a co-regulatory process at EU level, these should be voluntary. The use of such tools should be monitored closely as it can potentially interfere with EU citizens' fundamental rights to freedom of expression and information. Especially the obligation to ensure that the same piece of content is taken down and remains offline over time without a specific administrative or legal decision could put a disproportionate obligation on companies to police online content and the internet, in contradiction with the eCD's prohibition against general monitoring.

When requiring service providers to preserve terrorist content and related data for six months or more (Article 7), lawmakers risk imposing new data retention requirements on telecom service providers. This would increase legal uncertainty, given that no legal and harmonised framework is currently in place within the EU, and companies would be confronted with new financial and technical challenges.

b) Penalties

The introduction of a penalty clause in Article 18 is especially cumbersome as many of the factors to be taken into account for attributing a penalty are qualitative (e.g., transparency measures, complaint procedures and information to content providers). GSMA and ETNO recommend removing the notion of a financial penalty, and replacing it with cooperation between the main establishment of the provider and the authorities of that Member State on the listed parameters.

c) Application

Considering the complexity of the proposal and the need to cooperate with national authorities on a proportionate and effective order notification mechanism, hosting service providers should be given at least 12 months from the date of the regulation's entry into force to implement the final measures.

About ETNO
ETNO has been the voice of Europe's telecommunication network operators since 1992 and has become the principal policy group for European electronic communications network operators. Its 39 members and observers from Europe and beyond are the backbone of Europe's digital progress. They are the main drivers of broadband and are committed to its continual growth in Europe.
ETNO members are pan-European operators that also hold new entrant positions outside their national markets. ETNO brings together the main investors in innovative and high-quality e-communications platforms and services, representing 70% of total sector investment.

About the GSMA
The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.
For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.

Policy Contacts
Kristina Olausson
Policy Officer
olausson@etno.eu

Maria Sotiriou
Government Affairs Coordinator
msotiriou@gsma.com