GSMA ETNO Position paper on the proposal for a regulation on preventing the dissemination of terrorist content online

July 2019

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.

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.

Policy Contacts
Maria Sotiriou
Manager EU Affairs
msotiriou@gsma.com

Paolo Grassia
Director of Public Policy
grassia@etno.eu
Executive summary

- We invite co-legislators to support the amended wording in the Parliament’s text on Article 2 and Recital 10, clarifying that hosting services which satisfy at least one of the following criteria should be outside of the scope of the regulation:
  1. They do not communicate information to the public or give their users the ability to make such information available on the public Internet,
  2. They do not have contractual rights to control their users’ content,
  3. They do not have technical capability to remove individual end-user content, which usually goes hand in hand with not having contractual rights to control either.
- Based on these criteria, any exemption in the regulation for cloud computing should be technology neutral and futureproof. The exemption should be agnostic as to the cloud service layers, encompassing both PaaS (Platform as a Service), SaaS (Software as a Service) and IaaS (Infrastructure as a Service) where those cloud services satisfy the criteria above.

Intro

This document provides for GSMA and ETNO members’ position on the European Commission’s proposal for a regulation on preventing the dissemination of terrorist content online (TCR). GSMA and ETNO fully endorse the objective of the European Commission to tackle the dissemination of material that acts as incitement to violence and terrorism online. At the same time, we are concerned that the draft regulation as presented by the European Commission is too broad in terms of scope, and could unintentionally capture a number of services which do not meaningfully contribute to the dissemination of terrorist content online. It could also harm the offering of business-to-business cloud services, which is e.g. very crucial in the scope of industrial internet, including some of the cloud hosting services offered by our members.

In anticipation of forthcoming trilogue negotiations between the co-legislators, this position paper summarises the views of GSMA-ETNO members on the proposed regulation and calls on the Council and Commission to support the amended wording of the Parliament text. In particular, we ask that co-legislators endorse the Parliament’s proposed wording under Article 2 and Recital 10, narrowing the scope of the regulation to only include Hosting Service Providers whose services allow for the wide dissemination of terrorist material online, thereby focusing on where the vast majority of harm actually occurs. This also ensures that hosting services provided to businesses on specifically high safety standards, which do not allow the hosting service provider to control users’ content due to encryption, are excluded.

In so doing, we are confident co-legislators can deliver a targeted legal instrument which both satisfies the Commission’s original objectives, is technically workable and does not place undue limitations on the fundamental rights of EU citizens, such as the right to conduct a business. Such a solution would also enable businesses to offer secure cloud services in the scope of the industrial internet, and would create a disproportionate burden for service providers, who do not enable the dissemination of terrorist content online.
Our Role in Handling Content Online

GSMA-ETNO members are providers of mobile and fixed digital communications services across Europe, which provides us the opportunity to share practical experience in the handling of content. In large part, our services consist in the provision of electronic communication services (ECS) and Internet Access Service (IAS) to European consumers. As such, we are subject to a host of sectoral and horizontal regulation, governing the privacy and confidentiality of electronic communications transmitted over our networks and mandating that we cooperate with law enforcement agencies through data retention, lawful intercept and blocking access to sources of illegal material on receipt of a judicial order.

In addition, GSMA-ETNO members provide a variety of complementary and ancillary services that fall within the broad legal category of Information Society Services. Making use of our existing network capacity, IoT platforms and big data analytics, our members have developed a variety of value added professional IT services, encompassing managed cloud hosting (private, public and hybrid), cloud storage, digital transformation and storage optimisation services, co-location, application and infrastructure management, DDoS mitigation and security Information management.

Currently these services fall under article 14 of the eCommerce Directive, which establishes that hosting service providers should not be held primarily liable for the content they store and provide access to at the request of their users. Upon being notified of illegal content and thereby obtaining ‘actual knowledge’, such hosting service providers must act expeditiously to remove infringing material or risk losing their liability protections. The Terrorist Content Regulation as drafted by the European Commission would capture the hosting services provided by GSMA-ETNO members described above. However, there are a number of important technical characteristics of specific cloud services also provided by GSMA-ETNO members that we think justify their exclusion from the TCR. These cloud services provided by our members are typically chargeable (as opposed to ‘freemium’ and advertising funded services. We are concerned about unintended effects, which could affect GSMA and ETNO members’ services that in fact do not provide users with the capability to upload and share content with large audiences or the public. Given the broad range of proposed measures and related penalties, we believe that the scope should be more carefully targeted to not unduly affect services that only operate on the edge of the public web and exist for the purpose of the personal storage of content rather than the publication and dissemination of such content on the open Internet.

Regarding B2B, our members provide cloud hosting services (process capacity, storage and connectivity) where the customer exclusively manages the content and decides the structure and organization that they will have, as well as whether it is diffused. The ability of our members to remove a specific content is limited by several factors such as:

- The member company may not manage the service. In these cases, the cloud service provider has no access to the information itself and has only the capacity to block the service globally at the network layer. This would have the effect of having to close down a company’s access to all of its stored data.
- The structure and organization of the contents is done exclusively by the customer, as referred previously, based on encryption that technically prohibits control of the content by the cloud service provider.
The high safety standards that contractually and technically permit or prevent access by the hosting service provider to a customers’ data are crucial elements for the industrial internet. Particularly, business customers show a very high sensitivity concerning the safety of their data stored in the cloud. Trust in these services is key to stimulate service uptake in the EU, which is of strategic importance. Providers must therefore not be de facto prevented from continuously offering fully encrypted cloud services, which do not allow filtering or deleting of specific data by the service provider.

**A conditional rather than blanket exemption for cloud services**

We support the proposed exemption for cloud services in the Parliament’s text; however we do not support a blanket exemption for cloud services from the regulation. Rather we are in favour of an exclusion for cloud services that meet at least one of the following key criteria (for wording proposal see Annex I):

- Where the cloud service provider does not make material stored at the request of the user available to public;
- Where the cloud service provider has no contractual rights to control material stored at the request of the user, including how that material is structured or subsequently shared by its customers or by the end-users of such customers;
- Where the cloud service provider has no technical capability to remove individual, specified content by the customer or end-user of such customer, e.g. in case of encryption. This usually goes hand in hand with having no contractual rights to control the content.

**Current Wording of Parliament**

Based on these important technical considerations, it is our belief that the scope of the TCR should be more narrowly targeted as a clear subset of Hosting Service Providers. This change is necessary to ensure the regulation is technically workable, does not impair EU’s industrial internet that relies on secure cloud services and avoids placing a disproportionate burden on certain hosting providers, who do not enable users to disseminate material online.

The European Parliament recently voted through its report on the file, including an explicit exemption from the draft Regulation for 'cloud infrastructure and cloud services'. Accordingly, the Regulation "should not apply to cloud services, with respect to which the service provider has no contractual rights concerning what content is stored or how it is processed or made publicly available by its customers or by the end-users of such customers, and where the service provider has no technical capability to remove specific content stored by their customers or the end-users of their services" (Recital 10).

These amendments recognise the core issue: that to be effective and proportionate the provisions in this regulation should only apply to online content sharing platforms where terrorist content can be disseminated at scale to a very wide audience, and where the platform operator is actively involved in curating, optimising, promoting, tagging and suggesting content in order to drive ad revenue. In other words, content sharing platforms that play an active rather than passive role in disseminating content to the public.

By adopting a more targeted approach, additional regulation need only apply to those hosting service providers (HSPs) who actively manage their users’ content and, additionally, make terrorist content available to a very wide audience. It is our belief that this approach strikes an appropriate balance
between the rights and obligations of users and businesses on the one hand, and the imperative to protect EU citizens on the other.

**Technical neutrality between the cloud service layers**

Various drafts of the Parliament text included a specific exemption from the regulation for providers of ‘cloud infrastructure services’ (IaaS). While we recognise the intent behind this change, we are concerned that limiting the exemption to one specific cloud service layer goes against the principle of technological neutrality that should guide policymaking. Cloud computing is a generic term for the delivery of IT services over the Internet. These services are broadly divided into three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The three service layers are complementary and interdependent: the PaaS layer of the cloud is built on the IaaS layer of the cloud and is in turn used to build the most sophisticated layer of the Cloud: SaaS applications.

Many cloud service providers have a product portfolio spanning all three-service layers, and can offer tailored, scalable solutions that have elements of each. Owing to this fluidity, we think it is both artificial and counter-productive to enshrine within the regulation an exemption for one specific form of cloud service (“cloud infrastructure”). Such a narrowly drafted exemption would create an unfair regulatory safe harbour for providers of IaaS, especially as this is heavily dominated by a single US technology provider, distorting fair competition in the market for cloud services. Additionally, we think that such a narrow exemption would fail to allow for future market developments and technological innovations, where providers of IaaS look to combine elements of PaaS and SaaS in their product portfolio.

The proposed exemption for cloud services should be drafted in a technology neutral fashion, and should be flexible and adaptable to allow for market developments and technological evolution. Most importantly, the exemption for cloud should be conditional not on the service layer at which the cloud service sits. Instead it should be based on satisfying at least one of the three criteria included in the Parliament text: namely: i) where there is no communication to the public; ii) no contractual rights over end user content; or iii) no technical capability or granular control over end-user content.