# CISPE suggested amendments regarding the scope of the Proposed Regulation on terrorist content online

***UPDATED: 26th November 2018 -*** Cloud Infrastructure Services Providers in Europe (CISPE) welcomes the opportunity to provide its views on the European Commission's proposal for a Regulation on preventing the dissemination of terrorist content online (the "Regulation"). CISPE fully supports the intention and ambitions of the Regulation. However, including cloud infrastructure providers in the scope means **the wrong players are being targeted**.

Cloud infrastructure providers must be exempted from the Regulation. This needs to be clarified in the proposed law.

**SUMMARY**

(1) The Regulation targets the wrong player and needs to clarify that *cloud infrastructure service providers* are not in its scope:

- The Regulation is fitted for online content sharing services (e.g. social media and video sharing providers) and **not** for *infrastructure* service providers: online content sharing services **do** have control right down to the most granular piece of content made available on their platform by their users i.e. they ***can*** delete an individual comment, an image or target an individual end user - cloud infrastructure providers cannot do this: see (2) below.
- Cloud infrastructure providers are **not** social media, and they are **not** content sharing services providers. Cloud infrastructure providers are **NOT** controlling what content is put up, how that content is made available to the public, or to whom it is made available.
- What cloud infrastructure providers **ARE** is the underlying IT infrastructure: they are processors and not controllers. They provide the building blocks for cloud IT, analogous to power cables in the ground for a city, so enabling customers in business and government to build and run **their own** IT systems.

(2) Complying with the Regulation is technically not possible for *cloud infrastructure service providers*:

- It is not technically possible for a cloud infrastructure provider to take down or disable access to **one specific piece** of content because the infrastructure provider **does not have access** to the customers' content (which itself is the essence of the cloud infrastructure industry business model). This would be like asking a mechanic from the company that runs the motorway to repair a car that is running through it.
- Cloud Infrastructure as a Service (IaaS) providers cannot even distinguish what is "a piece of content" from what is not "a piece of content".
- For example, to take down a specific comment made public by a content provider a cloud infrastructure provider may need to take down the entire website in question, closing down access for related services and potentially a large number of other users, or even closing down of service of other customers.

(3) Imposing "automated proactive measures" to monitor or prevent uploads is not technically possible and would mean snooping all data that is not made available to the public

- It is impossible for the proposed law to result in monitoring the data of both public institutions (national governments, hospitals, law enforcement bodies, the EU Commission and Parliament) and corporate (lawyers, doctors, companies, banks, insurances…) that use our infrastructure and do not make content available publicly

- For some of large industrial customers who build trains, control airplanes or manage power plants using cloud infrastructure, this could undermine the security of there operations and trust in the service.
- If technical measures to prevent the upload of content were to be developed in the future, their application would contradict the Constitutions of a majority of Member States, since such proactive measures can be considered censorship.

CISPE urges the legislators to consider rules that are clear, workable and proportionate. Below is a more detailed review of aspects of the Regulation that are most concerning.

## 1. Scope and imposition of automated proactive measures (Core Request)

**1.1 Cloud infrastructure services should not be confused with online content sharing service providers: *the scope should be narrowed to 'online content sharing providers' that make terrorist content available to the public, not to third parties.***

Cloud infrastructure providers offer services that primarily include compute power, database storage and other related functionality. Often referred to as the "building blocks" for cloud IT, these services act as an initial layer of foundational infrastructure, enabling customers to build and run their own IT systems and end user services, which are designed, controlled and managed by such customers.

Third parties may include B2B customers (car manufacturers, electricity companies, research centers) contractually engaged with cloud infrastructure providers that are not end-users. Therefore "making content available to the public" is more suited than "third parties". Only the *customers of cloud infrastructure providers* (e.g. a social media company purchasing services from cloud infrastructure providers) have control and responsibility over their own data and the services they operate on top of the cloud infrastructure. Unlike with *social media platforms, video streaming services, video, and image and audio sharing services (Recital 10)* often referred as Software as a Service (or "SaaS"), cloud infrastructure providers **do not** access their customers' data and content and they **do not have general control** over what individual data is used, **when and if an individual content provider makes specific data available to the public** or who has access to it. Indeed, "***only those services for which the content provider is the direct recipient are in scope."*** Many information society services that the European Commission seeks to include in the scope of the Regulation are built on top of cloud infrastructure services.

When the Commission defined hosting services providers the key issue is whether the content is shared with third parties. Additionally, the storage should not be relevant since all providers entail a sort of storage of the data. In the context of cloud infrastructure, third parties refer to any customer of the cloud provider (for instance another business) and not the end customer or the public. Please see the infographic below explaining this issue.

*We urge co-legislators to narrow the scope to 'online content sharing providers' that make terrorist content available to the public and therefore exclude those providers that have no general control of and access to the content such as cloud infrastructure service providers.*

**1.2 As a cloud infrastructure provider, it is not technically possible to take down one specific piece of content, because the infrastructure providers do not have access to their customers' content.**

Cloud infrastructure providers and CISPE members are respecting existing laws and cooperate with judiciary authorities to fight terrorism. However, it is **technically impossible** for cloud infrastructure providers to identify and take down/block specific individual content as suggested by the Regulation, with any actions taken also having a potentially far broader impact than intended.

To take down a "piece of content", the cloud infrastructure service provider would have to "turn off' entire public services that rely on their infrastructure; including access for related other services.

For example: If an infrastructure customer is hosting social media or a website sharing content from 1,000,000 users and one user uploads a piece of illegal content, like a photograph, the infrastructure provider would be forced shut down the entire social media service or website. In reality, cloud infrastructure providers cannot even distinguish what is "a piece of content" from what is not "a piece of content". The Regulation incorrectly includes cloud infrastructure providers in its definition of a "hosting service provider".

**1.3 Implementing "automated proactive measures" – such as monitoring of data storage that use cloud infrastructure services as their building blocks – is not technically possible by cloud infrastructure providers**

Despite claims by filtering technology vendors, the filtering 'hashing recognition' technology used by social, video, image or audio sharing platforms, which creates a digital fingerprint of content that must be already identified (and made available to the public at least once) so the same content is not re-uploaded in another platform, cloud infrastructure providers are **not technically able** to use such technology since they do not have visibility or access over the content. This is not about providers going against their own terms and conditions but the technical reality that cloud infrastructure providers **do not** have access to review content, whether encrypted or not, nor even know the purpose of the content that end users may have (see CISPE Data Protection Code of Conduct[1] cispe.cloud). This stands in stark contrast to online content sharing services and platforms that **do** have access and control right down to the most granular piece of content on their platform i.e. they ***can*** delete a specific individual piece of content made available to the public or target an individual end user.

The entire business model of cloud infrastructure services providers is based on trust. Snooping all data of large industrial customers who, for example, build trains, planes or power plants may undermine their security and therefore their trust in the service. This Regulation could potentially lead to the end of cloud infrastructure services, and hinder competitiveness of European industries and services worldwide.

The Regulation also arguably contradicts the Constitutions in several Member States, since automated proactive measures could be considered censorship hampering free speech. The risk is that companies over-remove various lawful content faced with the fear of having fines imposed on them.

Existing European law does not allow Member States to impose a general obligation on hosting service providers to monitor the information that users transmit or store. However, in the Regulation the Commission argues that, given the "grave risks associated with the dissemination of terrorist content", states could be allowed to "exceptionally derogate from this principle under an EU framework". This exception could trample other fundamental rights including citizens' rights to privacy and freedom of expression.

*We urge the co-legislators to conduct a legal analysis on the proportionality and compatibility of the Regulation and the E-Commerce Directive[2].*

1 https://cispe.cloud/code-of-conduct/

2 Art. 14 and 15 of the E-Commerce Directive

## 2. *The Regulation puts the SME community at risk*

The Regulation would have a serious impact on all cloud infrastructure providers – not least as it is technically impossible to meet the requirements – including a rapid and notable impact on cloud infrastructure service providers that are SMEs. Such an effect would contradict ongoing strategy and efforts by EU institutions to support SMEs as the "backbone" of Europe's economy. SMEs could simply not afford the level of investment the legislation will require if passed (and, once again, bearing in mind that effective implementation would not be technically possible). The Regulation seems to aim to facilitate concentration and oligopolistic situation on the European market, developing huge barriers to enter the market that would be an issue first for European SMEs.

*We urge co-legislators to take into consideration the further impacts of the Regulation for SMEs.*

## 3. A one-hour timeline for content removal is not technically achievable for cloud infrastructure providers, including SMEs

The one-hour timeline for removal will not always be achievable for cloud infrastructure providers. While terrorist content should be removed expeditiously by the controller of that content, placing a strict deadline such as the one set forth in the Regulation will result in content being removed unnecessarily and could have broader impact than intended. Moreover, SMEs providing cloud infrastructure services do not necessarily have the 24/7 staff required to achieve content removal in such narrow timelines.

The one-hour deadline for content removal does not take into consideration the need for a cloud infrastructure provider to contact its customer, who is the controller of the content. The content controller should be the recipient of any order to remove content as they are the party responsible for the content and who has the ability to remove or restrict the content being made available. Indeed, the one-hour deadline for content removal does not take into account many difficulties to comply for example, the need to translate the request or identify whether the request comes from a valid competent authority, the technical operations to remove the content or the need to escalate the request internally.

*Instead, the deadline for companies to comply should be 'without undue delay' similarly to the obligation in the General Data Protection Regulation.*

## 4. The definition of "terrorist content" is unclear and subject to interpretation

The definition of terrorist content in the Regulation is unclear and can vary across Europe. While some types of content can be identified easily as illegal, others require nuanced legal judgment, which cannot be left to the discretion of a provider and therefore may require a judicial intervention. The legality of a specific piece of content may depend upon the context in which it is presented as well, and the cloud infrastructure provider is not in a position to evaluate context. For example, a video of a terrorist act may be considered illegal if it is in the context of recruiting people to commit terrorist acts. However, *the exact same video* may be being stored by a news organization for journalist purposes, or by researchers, or by a law enforcement agency conducting an investigation. We seek a clearer definition of terrorism to have legal certainty. Requiring cloud service providers to make judgments as to the legality of content places them in the role of law enforcement. Cloud infrastructure providers do not have the appropriate expertise to carry out this role. In addition, for smaller providers operating locally, a translation of the content in English or the language of the country where such provider operates may be necessary to simply identify which content is considered illegal.

*Companies would require a sole definition of terrorist content across Europe in order to be able to comply with the legislation in every country they operate, as well as in any Member State issuing a removal and referral order.*

**5. The competent authority at Member State level should be a single judicial authority**

The industry requires a single European point of contact that they can rely on and which enables them to swiftly address the requests made to remove content, this could potentially be Europol. A single point of contact would build trust in the authorities and would therefore speed up the way the companies could respond to the request. It would also be much more practicable than having to manage 28 or more competent authorities, which would be very complex and would place a particular burden on SMEs.

In order to facilitate the work of this single point of contact, each Member State should appoint one single judicial competent authority. We believe a judicial authority is better placed to assess these kinds of requests, rather than an administrative or law enforcement bodies due to the importance of fundamental rights that are stake. Having multiple authorities or non-binding authorities will make it more difficult for information services to evaluate and reply in a timely manner because they will need to apply high judgement as to the adequacy of the request and evaluation of the material.

Moreover, removal orders should be transmitted in the langue of the choice of a provider, to enable SMEs to understand properly any request and be able to react faster.

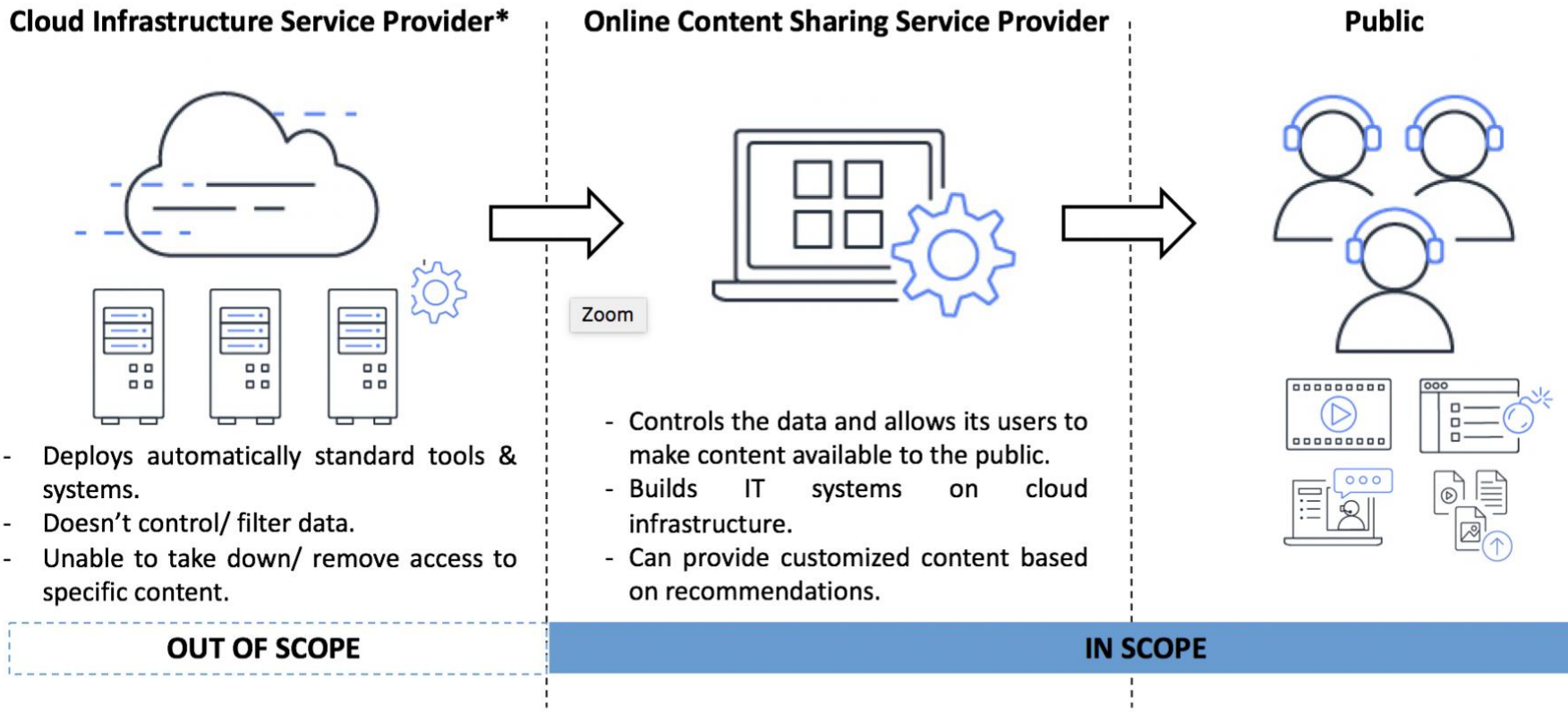
*To the extent that content is required to be removed by law, each Member State should have a single judicial authority that notifies the information society service that content must be removed.*

**6. Grounds for challenging removal orders should be revised**

There is a risk that removal orders could be misused in ways that pose a potential threat to EU fundamental rights. Currently, the Regulation requires companies to hire a local law firm if it does not already have resources in the country to challenge a request; this is extremely burdensome and would in practice prevent companies from being able to challenge removal orders in practice.

*We urge co-legislators to include a detailed due process in the legislation, especially to challenge removal orders.*

# Proposed scope for Terrorist Content Online Regulation




*Cloud Infrastructure Service Providers are providers of physical or virtual resources with self-service provisioning and administration on demand which provide application, infrastructure or platform capabilities and therefore have no general control of and access to information provided by online content providers.