September 5, 2022

CISPE position paper on the European Commission's Proposal for a Regulation laying down rules to prevent and combat child sexual abuse ("CSA")

Cloud Infrastructure Services Providers in Europe ("CISPE") welcomes the opportunity to provide its views on the European Commission's Proposal for a Regulation laying down rules to prevent and combat child sexual abuse material ("the Regulation"). CISPE fully supports the intention and ambitions of the Regulation. However, CISPE and its members wish to highlight cloud infrastructure's unique role in the fight against Child Sexual Abuse Material (CSAM). Ensuring that cloud infrastructure is treated relative to its position in the tech stack will be central to ensuring a proportionate and secure response to the scourge that is CSAM. We stand ready to discuss these concerns in greater detail with co-legislators.

1. Clarify Detection obligations

Limit detection orders to entities with direct access to and control over the content**. Cloud infrastructure providers should not be deemed the appropriate party to detect CSAM.**

CISPE believes that cloud infrastructure providers are not positioned to receive or implement detection orders effectively. This is inappropriate for two reasons.

First, cloud infrastructure providers **do not control the content their customers host, nor do they have access to content at the layer where detection is applied**. Cloud infrastructure providers offer customers cloud-based services that primarily include compute power, and database storage. Serving as the "building blocks" for cloud IT, these services act as foundational Infrastructure, enabling customers to build and run their own cloud-based IT systems, which are designed, controlled and managed by the customer, often "data controllers" but also "processors". Such customers include interpersonal communications providers, gaming applications, financial institutions, hospitals, and governments, and they have complete control of and responsibility for the content of the services they operate. These customers have a direct relationship with the end users of platforms where CSAM may be distributed. In contrast, cloud Infrastructure providers serve merely as "data processors" or "sub-processors" roles and, as such do not have control over what the content is used for, who has access to it or any information on the activities or identities of specific individual users of a platform or service. Without such contact with the end-user, they cannot access content in a way that would allow for the application of a tailored detection order that would not go beyond what is strictly necessary to address a CSAM risk effectively. To avoid undue interference with fundamental rights and ensure the proportionality of the Regulation, data controllers, who have such relations with end-users, are the entities that can implement detection orders in an effective, expedient and privacy-preserving way.

Second, content which is stored in the cloud may contain a **customer's proprietary data or confidential customer records**. Cloud infrastructure providers do not look at their customer's content. Their customers rely on that contractual commitment and agree to take responsibility for the content they host using cloud services. Additionally, because of the security measures and confidentiality cloud infrastructure providers owe to their customers, customers are always given the option, and total control over, **their encryption preferences**. When customers choose to encrypt, their data is rendered useless and inaccessible without

CISPE – Cloud Infrastructure Services Providers in Europe ASBL
Avenue Louise 87, 1050 Brussels, Belgium | Contact: cispe@europa-insights.com | T: 32 2 502 65 80 | Website: https://cispe.cloud | EU Transparency Register: 041495920038-44

encryption keys. It would not be appropriate to force cloud infrastructure providers to detect or monitor, considering infrastructure hosts sensitive, secure, private, content to enterprise customers, the likes of government, financial and medical institutions.

Proposed solution: *Because cloud infrastructure providers are **accountable** and not **responsible** for the illegal content hosted on their infrastructure, detection orders should only be targeted at the players that **control** CSAM, or the data controllers. **CISPE proposes that detection orders be addressed to service providers, acting as data controllers as per the General Data Protection Regulation ("GDPR").***

2. Removal obligations

Ensure cloud infrastructure providers are issued removal orders as a last resort

CISPE and its members are aligned with the need to remove CSAM expeditiously. It is rarely 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' granular content. This is the essence of the cloud infrastructure business model. When cloud infrastructure providers receive removal orders, they must sometimes take down the entirety of a service, rather than the "specific piece of content". By analogy, this would be like shutting off the electricity to an entire building instead of a single apartment. It is thus much faster to issue removal orders to "data controllers", as to remove content, cloud infrastructure providers will be obligated to re-direct the order to their customers.

Proposed solution: *We suggest introducing a "**cascade approach**" to ensure that data controllers, those closest to the content, **are approached in the first instance of removal orders, and that the data processors should only be contacted as a last resort**. This is consistent with the approach taken **in Article 5.6 of the e-Evidence Regulation**[1] , which defaults data production orders to be directed to the "data controller", and also reflects the industry-aligned Trusted Cloud Principles, which outline cloud infrastructures providers' principles for engaging with Government requests for access to data. The industry-aligned Dutch Notice and Take Down Procedure also features such an approach.*

Consistently offer Hosting Providers the option to either 'remove or disable' CSAM

We would also like to point out that 'removal' and 'disable', while similar, entail slightly different obligations. Cloud infrastructure providers are more suited to disable content, largely because the word 'removal' implies that the content is removed from the internet entirely. It is technically impossible for a cloud infrastructure provider to ensure all copies have been eradicated.

Proposed solution: *We would thus ensure that the Regulation, where appropriate, applies the option to disable or remove by featuring 'removal **or** disable access' as is currently written in Article 1c consistently throughout the Regulation.*

3. Encryption

[1] Art. 5.6 of E-evidence Regulation (political agreement) "European Production Orders shall be addressed to service providers, acting as data controllers, in accordance with Regulation (EU) 2016/679. As an exception, where the data is stored or processed as part of an infrastructure provided by a service provider to a data controller other than natural persons, the European Production Order may be directly addressed to the service provider, processing the data on behalf of the controller, where: - the data controller cannot be identified despite reasonable efforts on the part of the issuing authority, or - a European Production Order or other request for the data addressed to the company might be detrimental to the investigation"

CISPE – Cloud Infrastructure Services Providers in Europe ASBL
Avenue Louise 87, 1050 Brussels, Belgium | Contact: cispe@europa-insights.com | T: 32 2 502 65 80 | Website: https://cispe.cloud | EU Transparency Register: 041495920038-44

Safeguard encrypted data hosted on cloud infrastructure
Given the importance of encryption for cloud infrastructure services and their customers, undermining customer data security, privacy and safety must be avoided.

Cloud infrastructure providers always **provide the opportunity for their customers to use and control encryption.** Users of cloud infrastructure services may always choose to encrypt any data hosted as part of a cloud service. Strong encryption, including end-to-end encryption, protects users' sensitive data – including individuals, corporations, and governments. Requiring providers to engineer vulnerabilities into products and services would undermine the security and privacy of customers' data and the information technology infrastructure. Governments should avoid any action requiring companies to create security vulnerabilities in their products and services.

Proposed solution: *We encourage the co-legislators to introduce additional* ***safeguards to ensure providers are not obligated to undermine encryption in order to comply with a detection order. This is particularly important where such encryption tools are provided as part of a cloud infrastructure service as such are used to protect the security and privacy of data critical to the functioning and*** *safekeeping of society.*

4. Risk Assessment

Introduce different criteria depending on the type of service and increase timelines
Cloud infrastructure providers stand ready to perform risk assessments to demonstrate how they enforce their terms and conditions. However, the role cloud infrastructure plays for online safety is limited to the robust enforcement of its clear terms and conditions. The Regulation, at the moment, does not provide cloud infrastructure providers with the legal certainty that, in its risk assessment, such providers are not under the obligation to assess the risks of their customers and end users. For example, should a social media platform be hosted as part of cloud infrastructure, the cloud infrastructure should not be expected to take on the specific nature and risks of said social media platform, only the risks associated with the services that cloud supplies.

CISPE would also like to point to the tight three month's deadline for submitting a risk assessment. Furthermore, updating risk assessments every time a new service is launched will keep companies issuing risk assessments as soon as a new service is introduced, which may hinder innovation.

Proposed solutions: *We suggest that the Regulation be amended to clarify that the risk assessments for cloud infrastructure providers* ***are limited only to the services offered by the cloud infrastructure, as opposed to those of its customers.*** *We also urge the co-legislators to give providers and the EU Center the necessary leniency in timelines to define their risk levels accurately. Finally, we suggest limiting red tape, maximizing the up-take of the risk assessment, and upholding the incentives for innovation should be updated* ***no more frequently than annually****.*

5. Liability

Introduce a broader "Good Samaritan" Clause

CISPE – Cloud Infrastructure Services Providers in Europe ASBL
Avenue Louise 87, 1050 Brussels, Belgium | Contact: cispe@europa-insights.com | T: 32 2 502 65 80 | Website: https://cispe.cloud | EU Transparency Register: 041495920038-44

CISPE and members wish to point to the lack of protections and safeguards around the existing liability provision of the Regulation. Currently, Article 19 only offers protection when providers perform the **necessary activities to comply** with the Regulation in good faith. However, this fails to afford hosting providers safe harbour concerning measures that may be undertaken either voluntarily or as part of compliance with another legal obligation.

Proposed solution: *We recommend the safe harbour language in Article 19 be expanded to clarify the conduct a hosting provider takes in the context of its obligations under the Regulation,* ***or beyond****, as long as compliant under the GDPR and ePrivacy, remains fully eligible for the safe harbour. The extension of this Good Samaritan clause would be crucial to offering cloud providers and other providers the security required to continue updating state-of-the-art technology designed to protect children online.*

6. The EU Centre

Ensure compatibility with the existing global framework

CISPE supports the Commission's ambition to strengthen the EU's infrastructural capacity to fight CSAM on a unified front. Companies globally are already reporting to the U.S. National Center for Missing and Exploited Children (NCMEC) and local and national hotlines. CSAM requires a globally unified approach to law enforcement. Therefore, it will be of the utmost importance that NCMEC and the future EU Centre align and avoid duplication in their reporting requirements and conflicts of law. Without such an alignment, the risk of non-compliance caused by legal uncertainty may increase. We would also like to point to the different approaches that exist amongst these hotlines when it comes to the definition of CSAM. Different definitions of what constitutes CSAM, grooming, and age of consent, amongst others, cause difficulties for companies to comply, and enforcement challenges for Regulators.

Proposed solution: *We encourage the EU, the U.S., and other countries with active hotlines to* ***engage in dialogue*** *to ensure that remedies are found to the potential conflicts of law. We also urge co-legislators to engage in dialogue with other hotlines, such as InHOPE. Cybertip, and IWF to align the definitions of CSAM and other related activities to ease compliance and enforcement burdens for all.*

7. Additional concerns

Limit the support to victims to the EU Center

Article 21 would have cloud infrastructure providers directly intake reports of alleged CSAM from victims. **Cloud infrastructure providers are ill-suited to validate claims of CSAM (e.g. age, non-consent) and respond in a trauma-informed manner** or to vet the minor status of victims. As providers of IT infrastructure, CISPE and members are far removed from any type of end-user, particularly children. It can be traumatizing for children or adults to re-visit past experiences of abuse, and we warn against issuing this role to companies, especially those that only provide infrastructure services, that are not trained to provide this support in a sophisticated manner.

Proposed solution: *We urge the co-legislators to* ***assign the role of working with potential victims to the*** **new EU Center**, which can then file validated reports with providers, following **the cascade approach** described above.

CISPE – Cloud Infrastructure Services Providers in Europe ASBL
Avenue Louise 87, 1050 Brussels, Belgium | Contact: cispe@europa-insights.com | T: 32 2 502 65 80 | Website: https://cispe.cloud | EU Transparency Register: 041495920038-44

Extend entry into force

CISPE and members are concerned over the **short applicability of this Regulation**. While we recognize the absolute necessity of unified rules to tackle the issue of CSAM, we recommend that the co-legislators extend the six months entry into force. New CSAM reporting rules, the establishment of processes to collect data for transparency reports, and preparation to comply with removal and blocking orders will require significant resourcing and effort and at least a year to implement.

Proposed solution: *We recommend that co-legislators extend the applicability of this legislation to at least **one year** to allow businesses to adapt to upcoming obligations.*

8. Conclusion and final recommendations

We support the Commission's efforts to address CSAM in Europe, and CISPE stands ready to engage with co-legislators on this matter. Cloud infrastructure providers are committed to performing their appropriate role to remove, disable and block CSAM where required. However, we urge co-legislators to consider the unique role played by "data processors" to ensure maximum applicability and proportionality.

About CISPE

Cloud Infrastructure Services Providers in Europe (CISPE.cloud) is a non-profit association that focuses on developing greater understanding and promoting the use of cloud infrastructure services in Europe. Members based in 14 EU Member States range from SMEs to large multinationals. CISPE members invest billions of euros in Europe's digital infrastructure and currently provide services to millions of customers, including organisations in multiple countries and locations outside the EU.

Security and data protection are cornerstones of the CISPE constitution. It was the first association in the EU to develop a dedicated GDPR-compliant Code of Conduct for Data Protection for the sector, aligning with strict GDPR requirements to help providers comply while bringing clarity to customers to help them select providers and build trust in their services.

CISPE has always aligned with EU values: since 2016 all services declared under the CISPE GDPR Code of Conduct offer customers the ability to opt for services that securely store and process data exclusively within the EEA. CISPE also co-chaired the cloud industry working group (European Commission) to develop codes of conduct for reversibility and data portability under the Regulation on the free flow of non-personal data.

CISPE – Cloud Infrastructure Services Providers in Europe ASBL
Avenue Louise 87, 1050 Brussels, Belgium | Contact: cispe@europa-insights.com | T: 32 2 502 65 80 | Website: https://cispe.cloud | EU Transparency Register: 041495920038-44