**Joint industry call for protecting encryption and limiting detection orders in the EU Regulation laying down rules to prevent and combat child sexual abuse**

September 6, 2023

The undersigned industry associations representing technology companies remain deeply committed to making the digital space safer for everyone and in particular to protecting children online. We firmly stand behind the European Commission's overarching objective to prevent and combat child sexual abuse.

As such, we believe certain improvements need to be introduced in the proposal for an EU Regulation laying down rules to prevent and combat child sexual abuse (CSA Regulation) in order to achieve a legislative framework that recognises our industry's efforts to safeguard children and one that better ensures the prosecution of perpetrators.

To this end, we call on EU policymakers to 1) **defend the rights to privacy and confidentiality of communications** through the specific protection of encryption; 2) **make sure that detection orders are a last resort measure**; and 3) **limit detection orders to those with the ability to act.**

## 1. Safeguard encrypted communications

Encryption (including end-to-end encryption of data) plays a key role in the provision of private and secure communications, including those of minors[1].

The importance of encryption technologies, and end-to-end encryption in particular, in safeguarding the security and confidentiality of users' communications is already acknowledged in currently applicable EU legislation[2] and should not be undermined by the CSA Regulation. Governments and public authorities rightly want to protect children from harm, but weakening encryption is the wrong approach and would put millions of EU citizens at risk of hacking, fraud and identity theft.

These risks have been highlighted by many actors[3], who have drawn attention to the privacy and security implications of scanning the content of encrypted communications to detect child sexual abuse.

The proposed Regulation fails to clearly exclude end-to-end encrypted services from an obligation to scan message contents and could instead mandate providers to deploy certain potentially invasive technological solutions – such as client-side scanning (CSS) – to execute detection orders. This would seriously undermine the robust protection that end-to-end

[1] As stated in UNICEF's White Paper on Encryption, Privacy and Children's Right to Protection from Harm, "Encryption is also critical to ensure children's safety. Their digital devices and communications contain personal information that could compromise both their privacy and safety if it fell into the wrong hands."

[2] Including in Regulation (EU) 2021/1232 (Interim Regulation on a temporary derogation of the ePrivacy Directive to combat online child sexual abuse), in Directive (EU) 2022/2555 (NIS 2 Directive) and in Regulation (EU) 2023/1543 (e-Evidence).

[3] Joint Opinion 04/2022 by the European Data Protection Board and the European Data Protection Supervisor and Open Letter by Academics and Researchers on CSA Regulation.

encryption provides to people's privacy and security, and increase the likelihood of unjustified privacy breaches. Cybersecurity experts have repeatedly warned that weakening any part of an encrypted system would decrease the safety and security of everyone, everywhere[4].

That is why the EU co-legislators should make sure that the obligations in the CSA Regulation are proportionate to the known risks and explicitly exclude any prohibition or weakening of encryption, including access by any third party to communications and digital data which are not meant to be accessed, read or edited.

In order to respect users' privacy and ensure childrens' safety, encrypted services should be permitted to tackle child sexual abuse without accessing message contents. This should include approaches like product design, the analysis of unencrypted surfaces, and metadata processing.

**2. Ensure that mandatory detection is targeted and issued as a last resort measure**

The CSA Regulation is an opportunity to build on existing efforts to fight against child sexual abuse. These well-established efforts include detection using high-quality databases of known child sexual abuse material (CSAM), voluntary prevention and detection measures, as well as the development of novel technologies. These tools already result in many actionable reports to law enforcement as well as in the successful prosecution of offenders worldwide. It is of the utmost importance that measures proven to be effective are preserved.

In this context, the CSA Regulation should ensure that the issuance of detection orders remains a last resort measure, enforced only after finding that the provider has failed to take all reasonable and proportionate mitigation measures to address the risk of their services being potentially misused for the purpose of online child sexual abuse. This approach would ensure continuity with existing targeted activity and support law enforcement authorities in investigating and prosecuting offences.

The proposal should therefore, first, enable providers to continue deploying proactive voluntary actions for the prevention, detection and removal of child sexual abuse as a mitigation measure under Article 4 and, second, ensure that detection orders are only activated once it is clear that a certain provider has failed to appropriately mitigate the risks.

Further, caution should be exercised for detection orders of previously unknown CSAM and the solicitation of children (so-called 'grooming'), given the technical and operational difficulties with detecting this type of content, which requires human confirmation and review of contextual communication[5].

To support this approach, the CSA Regulation also needs to provide clarity on how providers should implement the detection orders, while staying in line with the principle of no general

[4] Paper 'Bugs in our Pockets: The Risks of Client-Side Scanning'; Paper 'Keys Under Doormats: Mandating Insecurity By Requiring Government Access to All Data And Communications'; Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; Electronic Frontier Foundation explained 'Why Adding Client-Side Scanning Breaks End-To-End Encryption'; and Internet Society factsheet 'Client-Side Scanning'.

[5] As highlighted in the complementary impact assessment by the European Parliament Research Service.

monitoring or active fact-finding obligations, as recently reconfirmed in the Digital Services Act (DSA).

3. **Limit detection orders to providers with the ability to act**

The CSA Regulation refers to the term 'hosting service', which is very broad and encapsulates a variety of service providers with different technical and operational capabilities. For example, certain providers may use cloud computing services to store content uploaded by their users. In this case, both the service provider and the cloud hosting would qualify as 'hosting services' under this Regulation, even though cloud providers lack full visibility over users' content and are unable to apply detection orders in a way that is proportionate and safeguards privacy.

Requiring providers like cloud computing services to detect online child sexual abuse would show a disregard to their capabilities and disrupt the confidentiality of their customers' data, which could include businesses and governmental organisations. Co-legislators should introduce language in the CSA Regulation clarifying that detection orders should only be issued to those downstream providers with the technical and operational ability to act, so as to prevent and minimise any possible negative effects on the availability and accessibility of information, in line with Recital 27 of the DSA.

**Conclusions**

We, the below-mentioned signatories, fully support the proposal's objective to fight child sexual abuse, and to strengthen existing efforts and ongoing cooperation between national authorities. The new rules need to be proportionate and preserve the privacy of communications, while still allowing for innovation in the fight against child sexual abuse in the EU and beyond. To achieve this, lawmakers need to ensure that the proposal specifically protects encrypted communications and that detection orders are the last step of the process, targeting those providers with the technical and operational ability to act.

While time is of the essence, the CSA Regulation should not be rushed without carefully considering balanced and future-proof solutions to achieve its intended goals. Only this way a robust legislative framework that stands the test of time will be put in place.

The undersigned associations are eager to continue engaging with policymakers and other relevant stakeholders in order to secure ongoing and future efforts to combat child sexual abuse online, while at the same time safeguarding the fundamental right to privacy of EU citizens.

Signatories (in alphabetical order):

- AFNUM (Alliance Française des Industries du Numérique) - Registered in France under 438608630 (HATVP)
- CISPE.cloud (Cloud Infrastructure Services Providers in Europe) - 041495920038-44
- Computer & Communications Industry Association (CCIA Europe) - 15987896534-82
- CZ.NIC (Czech Internet Association) - Registered in the Czech Republic under 67985726
- Developers Alliance - 135037514504-30

- DOT Europe - 53905947933-43
- Eco (Verband der Internetwirtschaft e.V.) - 483354220663-40
- EuroISPA (European Internet Services Providers Association) - 54437813115-56
- FiCom (Finnish Federation for Communications and Teleinformatics) - 29762326480-22
- Freedom Internet - Registered in the Netherlands under 74768573
- i2Coalition (Internet Infrastructure Coalition) - 722865639438-43
- ISPA Austria (Internet Service Providers Austria) - 56028372438-43
- ITI (Information Technology Industry Council) - 061601915428-87