Joint industry call for protecting encryption in the Child Sexual Abuse Regulation

June 3rd, 2024

The undersigned industry associations representing various industries 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 (CSA).

Preserving the integrity of end-to-end encryption

In view of the latest developments[1] in the Council Law Enforcement Working Party and the strong political pressure surrounding discussions on the Child Sexual Abuse Regulation, the signatories **reiterate their call on the Member States to protect both safety and privacy in the Council position. That can only be done by preserving the integrity of end-to-end encryption** (E2EE) and not entertaining proposals that would jeopardise the privacy and confidentiality of communications for millions of Europeans, such as the suggested "upload moderation", which is just another form of client-side scanning (CSS), or similar suggestions.

Encryption technologies, including end-to-end encryption, play a crucial role in building trust in online services. Users are thereby guaranteed that none other than themselves and the recipients of their communications will be able to see the content shared. This technology is valued in currently applicable EU legislation[2] and has been defended in a landmark European Court of Human Rights ruling[3]. The risks posed thereto in the CSA Regulation have been highlighted many times already[4].

Suggestions that are currently on the table in the Council Working Party claim that E2EE data is not in scope of the detection orders because the detection is done via "upload moderation" (i.e. before the E2EE protocol is applied) and this upload moderation is subject to the consent of the user. However, this remains highly problematic for the privacy of users and the security of the internet, as it mandates providers to deploy certain potentially invasive technological solutions – such as CSS or server-side scanning – to detect images, videos and URLs. It also creates a new type of "consent" that we do not believe would be in line with EU legislation and CJEU jurisprudence[5].

We therefore urge Member States to discard any proposal that would mandate access by any third party to communications and digital data which are not meant to be accessed, read or edited, before or during transmission of such data or while the data is at rest.

---

[1] See here: https://netzpolitik.org/2024/internes-protokoll-belgien-will-nutzer-verpflichten-chatkontrolle-zuzustimmen/

[2] Including in Directive (EU) 2022/2555 (NIS 2 Directive) and in Regulation (EU) 2023/1543 (e-Evidence).

[3] *Podchasov v. Russia* App no 33696/19 (ECtHR, 13 February 2024). In this case, the ECtHR ruled that Russia's actions, specifically the decryption of private communications, violated the right to privacy as protected under Article 8 of the European Convention on Human Rights.

[4] Including in the Joint Opinion 04/2022 by the European Data Protection Board and the European Data Protection Supervisor and in the Open Letters by Academics and Researchers on the CSA Regulation (July 2023 and May 2024).

[5] Users will be forced to or be coerced to consent as the absence of such consent will eventually mean that they cannot use the service in full.

Ways forward to improve the proposal

The proposal can be improved to the benefit of all users, including children, by **enabling the proactive processing of personal and other communications data, which includes voluntary detection and prevention, by all number-independent interpersonal communication service (NIICS) providers in order to tackle CSA on their services**. This would minimize the risk of CSA use of their services and would be consistent with Article 3 on risk assessments. Voluntary detection in NIICS is currently legally possible under the ePrivacy derogation[6] and enables companies to deploy, with safeguards, detection technologies responsible for the tens of millions of reports of CSAM made to authorities in 2022 alone.

Additionally, several other points must be resolved before a final agreement can be reached among Member States. Policymakers should consider targeting requirements at the right points in the ecosystem, i.e. at entities with a direct relationship with the user, as opposed to infrastructure providers which have less capacity to act. The scope should be narrowed down to capture only service providers that are best placed to take effective mitigation and enforcement measures and exclude number-based interpersonal communication service providers.

While we recognise the importance in reaching a deal on this text soon, the CSA Regulation must be carefully crafted to ensure balanced and future-proof solutions. Only such an approach will create a robust, enduring legislative framework. Our associations are committed to engaging with policymakers and stakeholders to combat child sexual abuse online while protecting EU citizens' privacy rights.

Signatories:

ACT – The App Association - 72029513877-54

AFNUM (Alliance Française des Industries du Numérique) - 832852453029-02

Computer & Communications Industry Association (CCIA Europe) - 281864052407-46

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

ITI - The Information Technology Industry Council - 061601915428-87

[6] Regulation (EU) 2021/1232 (ePrivacy derogation)


ACT | The App Association
ccia
Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.


AFNUM


DOT.
europe
Digital • Online • Tech


eco
VERBAND DER INTERNETWIRTSCHAFT


EuroISPA


FiCom


ITI