defend|digital|me

October 7, 2024

We write from Defend Digital Me with reference to the discussion of EU government positions on the Hungarian proposal about the CSA Regulation planned for this Wednesday, October 9th.

We published a report in 2023 together with Child Rights International Network (CRIN), ***Privacy and Protection: A children's rights approach to encryption***.[1] After a year in research together with leading stakeholders from a wide range of European, U.S. and other global organisations, including many working with children for their protection and law enforcement, we concluded that such proposals breach the long-standing principle of the protection of confidentiality from mass monitoring. Protecting privacy is key to protecting children's full range of rights, with consequences for children's democratic participation in society, access to information, and ability to seek safety in confidential spaces.

These proposals will not achieve the aims of reducing harm to children from CSAM. Instead the proposals harm human rights and fundamental freedoms, democracy and the rule of law. We already joined a statement in July 2024[2] with EDRi and 48 digital rights, human rights and children's rights/ protection organisations to ask that this proposal is opposed as it stands. From our own decade of research of school surveillance technologies, we are deeply concerned that today's mass digital monitoring is exposing children's private messages and consensual content between teenagers, giving **commercial companies' staff access and retention of "nudes".**

The UN Committee on the Rights of the Child, General comment No. 25 (2021) states, "Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge".[3]

The European Commission must withdraw the draft CSA Regulation and instead participants should agree on a joint list of necessary revisions.

1) **No indiscriminate scanning: Instead of mass monitoring of messaging and online activity, law enforcement should pursue primary prevention, and order digital searches only of suspects;**
2) Member States must **invest in the capacity and resources of national child protection** support;
3) **Protect secure encryption:** client-side scanning to infiltrate encryption must be ruled out;
4) **Protect anonymity: Remove mandatory age verification** by all communications companies and services to save the right to communicate anonymously and **protect secure participation.**

We have three grave areas of concern; **fundamental rights and freedoms** of individuals and communities; personal and national **security risks at scale**; and the national and international **threat to democracy** that comes from undermining both the principle and substance of practice that these proposals introduce in a radical shift from which there will be no return.

These proposals will not better protect children. In fact it puts them at new risks. Why? Using resources to keep looking for volumes of recurring known material does not save children from ongoing abuse,

[1] Privacy *and* Protection: A children's rights approach to encryption. (2023) Child Rights International Network and defenddigitalme. https://home.crin.org/readlistenwatch/stories/privacy-and-protection

[2] On 1 July, EDRi and 47 civil society organisations sent a joint statement to the Hungarian Council Presidency and a number of member state permanent representatives https://edri.org/our-work/joint-statement-on-the-future-of-the-csa-regulation/

[3] UNCRC GC25 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[redacted]

but instead diverts resources needed to investigate contact abuse. It also diverts meaningful company accountability and replaces it with tick-box compliance.

Children are just as much entitled to the **right to privacy** that should defend their right to respect for their own private and family life, home and *correspondence* (Article 8 ECHR). Some wrongly claim these proposals do not breach privacy. The Council Legal Services disagrees, finding that the proposals violate fundamental rights[4] through the "particularly serious limitation to the rights to privacy and personal data protection enshrined in Article 7 and 8 of the Charter".[5]

Others wrongly claim that monitoring for content screened only using AI, client-side, or non-human scanning does not breach privacy. But all services are ultimately controlled by people who, if access is mandated, can grant inappropriate access to others, including for commercial interests, to meet any State demands, or even after blackmail or hacking.

Indiscriminate mass surveillance and back-dooring of encrypted communications also opens up a raft of **grave national, governmental, and personal security risks** shown by the news most recently that AT&T and Verizon are among the **US broadband providers whose networks have been breached in a cyberattack tied to the Chinese government**, accessing information via systems the federal government use for court-authorised network wiretapping requests.[6] European networks and all of our communications will become similarly vulnerable to such attacks if the proposals go ahead.

Furthermore, to ignore **the European Data Protection Board joint opinion** [7] warning the legislative plan raises "serious data protection and privacy concerns," is to ignore our **rule of law on data protection**.

It is a key principle of European democracy that fundamental rights can only be infringed where *lawful*, *necessary and proportionate*, but these proposals dis-apply this longstanding position. As a leading global model of democracy and freedoms, for the EU to lose this global position will not only be detrimental for our press, defenders of rights and freedoms, and political protestors including children and young people around Europe, but around the world, as other leaders will copy the anti-democratic change to disregard not only data protection laws but wider fundamental human rights.

If this goes ahead it will be a dangerous step in the acceptance of other authoritarian measures that says to the world that fundamental rights and freedoms are something optional. What other principles in future will be viewed as being at the discretion of the political leaders of the day, with particular partisan agendas and without any democratic mandate of the people they serve?

I ask for your support and thank you for your consideration.

Sincerely,
Jen Persson, Director, Defend Digital Me [redacted]

[redacted] | w: http://defenddigitalme.org/ | Twitter @defenddigitalme
Defend Digital Me is a call to action to protect children's rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education.

---

[4] In a 2024 milestone judgment—Podchasov v. Russia—the ECtHR ruled that weakening of encryption can lead to general and indiscriminate surveillance of the communications of *all* users and violates the human right to privacy. https://hudoc.echr.coe.int/eng/?i=001-230854

[5] Council Legal Service opinion (2023) https://www.statewatch.org/media/3901/eu-council-cls-opinion-csam-proposal-8787-23.pdf

[6] WSJ (October 5, 2024) https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b U.S. Wiretap Systems Targeted in China-Linked Hack

[7] EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

[redacted]