Open letter by the Internet Society, supported by cross-group Members of the European Parliament, to Interior & Justice Ministers of EU27, calling for strong end-to-end encryption as part of the Regulation laying down rules to prevent and combat child sexual abuse.

Brussels, 17 October

Re: Call for strong end-to-end encryption as part of the Regulation laying down rules to prevent and combat child sexual abuse.

Dear Minister Laanemets,
Dear Director Jaarats,

In representation of the Internet Society, and supported by Members of the Parliament, we are writing to express our deep concerns regarding certain proposed measures in the Regulation laying down rules to prevent and combat child sexual abuse[1] (CSA Proposal) that could impact the security and privacy of European citizens and businesses. This letter focuses on **encryption and the use of client-side scanning technologies** but is notwithstanding other concerning issues raised by the proposal, like the untargeted scanning of private conversations of innocent and unsuspected individuals.

We want to draw your attention to the language in the Commission's proposal and in the latest available Council's compromise text proposed by the Spanish Presidency that **effectively weakens protections** for the use of end-to-end encryption. Using the proposed language would harm EU citizens, including the children this law aims to protect.

Therefore, **we urge you to carefully consider the consequences of these measures and to support a text that clearly and explicitly protects against the prevention, weakening of, or undermining the use of end-to-end encryption, nor deducing the substance of the content of the communications including through Client-Side Scanning.**

Encryption is a crucial technology which serves as a foundation for safeguarding individuals, their data, and their communications, ensuring privacy and security, including for government secure communications and for business secrets. It is essential that decrypted data can only be seen and read by the two endpoints in conversations - the sender and the intended recipient. Any loss or weakening of secure end-to-end encryption (E2EE) would create new vulnerabilities that would put millions of European Internet users, public services, journalists, and businesses at risk.

While we understand that some governments and policymakers view E2EE as a hurdle for law enforcement, it is paramount to recognize that systematically weakening individuals' digital safety is not the solution. E2EE represents the gold standard of security and privacy in our increasingly digital world, and it is crucial that we push back against any efforts to undermine it.

Furthermore, while the objectives of the CSA Proposal of facilitating law enforcement agencies' work are commendable, it is vital to consider the potential consequences. There are no feasible technical solutions that enable service providers to maintain end-to-end encrypted services while meeting the detection responsibilities outlined in the proposal. **These solutions simply do not exist.** This places providers in a challenging position,

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN, Published on 11 May

internetsociety.org
@internetsociety
Rue Vallin 2
Geneva, CH-1201 Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
11710 Plaza America Dr, Suite 400,
Reston, VA 20190 USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881

where they must choose between eliminating encryption entirely or offering a compromised version of their services.

We are also concerned by the ongoing discussions surrounding the use of client-side scanning technologies to achieve the objectives of the CSA Proposal. There is a common misconception that robust E2EE can coexist with client-side scanning before encryption. In fact, client-side scanning **undermines the very essence of encryption itself.**

The following analogy can help clarify the misconception: ***breaking encryption is opening a sealed letter and reading the content before it arrives to the recipient; client-side scanning is having somebody looking over your shoulder while you write the letter.*** The purpose of encryption is fundamentally undermined, as well as all its benefits.

The European Parliament's Complementary Impact Assessment[2] also states that moving from server-side to client-side scanning **creates new vulnerabilities** to attacks even if the devices are regularly updated to fix security issues. These vulnerabilities can be exploited by various entities, including governments, non-state actors, and foreign adversaries, weakening the overall information infrastructure. Moreover, there is a risk of abuse associated with client-side scanning. Even though scanning applications are intended to detect only child sexual abuse materials, there is a possibility that these parameters could be altered in the future to monitor additional applications or behaviours through the device, causing a spill-over effect to other domains.

As stated in the EDPB-EDPS Joint Opinion,[3] client-side scanning "can be **easily circumvented** by encrypting the content with the help of a separate application". The consequence is clear: tech-savvy perpetrators will evade the measures and the masses of innocent users of E2EE services alone in the face of compromised services and imperfect data protection rights.

In short, client-side scanning creates new vulnerabilities and abuse risks, can be circumvented, and undermines the core purpose of encryption: these techniques are totally inefficient to solve the societal problem they intend to address. Should it be introduced in EU law, it could open the door to other breaches of encryption and have broader impacts.

Now, more than ever, and in line with the Parliament's 2022 position[4], it is crucial to unequivocally demonstrate your support for encryption as a technology designed to:

- Empower individuals to connect with like-minded peers and establish online communities.
- Allow individuals to exercise their fundamental rights, safeguard their privacy, and protect the lives of their loved ones.
- Provide a secure haven for those in need of assistance, enabling them to communicate without fear or apprehension.
- Act as a digital shield for children's online activities, fostering a secure environment for them to explore, share, and learn. This assurance extends to parents and

[2] https://www.ecorys.com/sites/default/files/2023-05/EPRS_STU%282023%29740248_EN.pdf, Proposal for Regulation laying down the rules to prevent and combat child sexual abuse, Complementary impact assessment, Published in April 2023

[3] https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en, 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, Published in April 2022.

[4] European Parliament resolution of 7 July 2022 on the US Supreme Court decision to overturn abortion rights in the United States and the need to safeguard abortion rights and women's heath in the EU (2022/2742(RSP)), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0302_EN.html

guardians, who gain peace of mind knowing that their children's privacy is respected and protected online.
- Protect law enforcement and national security communications from infiltration and espionage.
- Enhance the security of organizations operating in the digital realm, ultimately promoting innovation and economic growth for businesses of all sizes, both locally and globally.

Against this background, **we urge you to carefully weigh the potential consequences and implications of the proposed measures before signing off on the Council's General Approach** to the CSA Proposal and prioritize the security, privacy, and fundamental rights of European citizens.

We look forward to your response.

Yours sincerely,

David Frautschy
Senior Director for European Government and Regulatory Affairs

The Internet Society, with the support of the undersigned Members of the European Parliament.

MEP Alex Agius Saliba (Malta)
MEP Andrus Ansip (Estonia)
MEP Cornelia Ernst (Germany)
MEP Malte Gallée (Germany)
MEP Markéta Gregorová (Czechia)
MEP Marcel Kolaja (Czechia)
MEP Karen Melchior (Denmark)

The Internet Society is an organization that was founded more than 30 years ago by some of the Internet pioneers, with the mission to support and promote the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society. The work of the Internet Society aligns with the goals for the Internet to be open, globally connected, secure, and trustworthy.