Saatja: David Frautschy <frautschy@isoc.org>
Saadetud: 17.10.2023 23:47
Adressaat: <klen.jaarats@riigikantselei.ee>; <lauri.laanemets@riigikantselei.ee>; SiM info <info@siseministeerium.ee>; <lesli.hommik-callewaert@mfa.ee>
Koopia: Carl Gahnberg <gahnberg@isoc.org>; Callum Voge <voge@isoc.org>
Teema: MEPs and Internet Society open letter - Support for strong end-to-end encryption
Manused: image001.png; Letter to the EU Interior Ministers_Estonia.docx

TÄHELEPANU! Tegemist on väljastpoolt asutust saabunud kirjaga. Tundmatu saatja korral palume linke ja faile mitte avada!

Dear Minister Laanemets,
Dear Director Jaarats,
Dear Counsellor Hommik-Callewaert,

In representation of the Internet Society, and supported by Members of the Parliament, I am attaching an open letter expressing our deep concerns regarding certain proposed measures in the Regulation laying down rules to prevent and combat child sexual abuse (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 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 of the use of, end-to-end encryption (E2EE), nor deducing the substance of the content of the communications including through Client-Side Scanning.

Despite the information you may have received in the past, there is broad technical consensus that 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**.

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. 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 EDPB-EDPS Joint Opinion and the European Parliament's Complementary Impact Assessment also defend that the proposal from the European Commission is not fit for purpose.

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.

On behalf of the Internet Society, and 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 (Dennmark)

--
David Frautschy Heredia, Senior Director for European Government and Regulatory Affairs
frautschy@isoc.org

Lingitud pilti ei saa kuvada. Võimalik, et fail on teisaldatud, ümber nimetatud või kustutatud. Veend

internetsociety.org | @internetsociety
Join the global movement today
Together we can protect the Internet of tomorrow