

(English version)

Question for written answer E-003249/25
to the Commission
Mathilde Androuët (Pfe)
(17 August 2025)

Subject: Proposed chat control measures: risks to privacy and encrypted communications

Social media users in the Member States have expressed serious concerns ⁽²⁾ over the proposed chat control measures that would introduce the widespread scanning of encrypted messages in order to tackle child sex abuse material ⁽¹⁾. While the objective is of course commendable, the EDPS ⁽³⁾, many tech companies, cybersecurity experts and digital rights associations ⁽⁴⁾ believe this measure will open the way for widespread mass surveillance, threatening the privacy and freedoms of EU citizens. The Signal Foundation states that it might be forced to leave the EU market to avoid compromising the encryption of its service ⁽⁵⁾.

1. Can the Commission ensure that this proposal complies with the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 (on privacy and personal data protection) thereof?
2. How will it safeguard the integrity of end-to-end encryption as a pillar of digital security?
3. Have the impact assessments taken proper account of the high risk of false positives, which could have serious consequences for innocent citizens?

Submitted: 17.8.2025

Answer given by Mr Brunner on behalf of the European Commission
(5 November 2025)

Communications companies are the main actors capable of detecting explicit videos or videos that are child sexual abuse material. Currently they are encouraged to do this voluntarily — a practice that has existed for over a decade and proved essential for child protection. Many major investigations in recent years have been made thanks to this approach.

The Commission proposal for a regulation to prevent and combat child sexual abuse ⁽¹⁾ seeks to make this approach mandatory. The proposal is clearly defined, the terms are closely monitored by data protection authorities and provide guarantees. A similar approach is already being widely used to detect malware and spam.

The proposal includes provisions on detection orders, which are measures of last resort when prevention measures are insufficient. They target only high-risk services, or, where possible, specific users or groups.

Such orders are issued by a judicial or independent administrative authority balancing all the rights at stake and after a thorough assessment of their necessity and proportionality.

The proposal is technology neutral, while acknowledging encryption as an important tool to guarantee the security and confidentiality of the communications of users.

When executing a detection order, providers are required to put in place the requisite safeguards to ensure the security and confidentiality of the communications of users.

The impact assessment ⁽²⁾ analysed and assessed the risk of false positives, which for some technologies is estimated at no more than 1 in 50 billion ⁽³⁾.

Nonetheless, the proposal includes safeguards to address such risks, including requiring providers to deploy technologies that are the least privacy-intrusive in accordance with the state of the art in the industry, and that limit the error rate to the maximum extent possible, as well as judicial redress if needed.

² “Voilà les pays de l’UE qui abandonnent la vie privée pour scanner vos messages chiffrés”, Melina Loupia, 3 August 2025, <https://www.clubic.com/actualite-574944-voila-les-pays-de-l-ue-qui-abandonnent-la-vie-privee-pour-scanner-vos-messages-chiffres.html>

¹ COM/2022/209 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209>

³ European Data Protection Supervisor, 28 July 2022

⁴ “Tech Firms Warn Against EU Chat Control”, Emma Woollacott, 22 January 2024, https://www.forbes.com/sites/emmawoollacott/2024/01/22/tech-firms-warn-against-eu-chat-control/?utm_source=chatgpt.com

⁵ “EU Chat Control Proposal to Prevent Child Sexual Abuse Slammed by Critics”, Mihir Bagwe, 18 June 2024, <https://theycyberexpress.com/eu-chat-control-proposal-slammed/>

⁽¹⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209>.

⁽²⁾ *Ibid.*

⁽³⁾ <https://www.congress.gov/116/meeting/house/110075/witnesses/HHRG-116-IF16-Wstate-FaridH-20191016.pdf>.