

(English version)

**Question for written answer E-003993/25
to the Commission
Mary Khan (ESN), Petra Steger (PfE)
(11 October 2025)**

Subject: EU Chat Control plans may prompt Signal app to pull out of Europe

On 1 October 2025, Meredith Whittaker, the president of Signal — considered the most secure messaging app currently available — spoke to the German Press Agency (dpa), criticising the EU for its Chat Control plans. As part of these plans, messaging services would be forced to introduce backdoors that allow for private communications to be automatically screened for potential criminal content. This screening would be carried out before the data has even been encrypted. Whittaker stated that if worst comes to the worst, Signal will work together with its partners and the community to find ways around these rules, just like what happened in Russia or Iran with the state-wide blockades. However, if it has to choose between maintaining end-to-end encryption and remaining in the European market, Signal will ‘unfortunately decide to withdraw from Europe’ ⁽¹⁾.

1. What view does the Commission take of the Signal president’s well-founded criticism of the Chat Control plans and the impact they may have on data protection, IT security and EU citizens’ fundamental rights?
2. How does the Commission justify the fact that the planned Chat Control may force an internationally recognised, secure messenger app to discontinue its services for all EU citizens?
3. How does the Commission view the fact that the EU regularly and strongly condemns the surveillance methods of authoritarian regimes, such as those in Russia and Iran, yet it is effectively stooping to their level by preventing Signal from acting as a secure messaging service?

Submitted: 11.10.2025

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(23 December 2025)**

The Commission has taken note of the views expressed by Signal regarding the proposal for a regulation to prevent and combat child sexual abuse ⁽¹⁾.

The proposal focuses on prevention and includes provisions on detection orders as measures of last resort when prevention measures are insufficient; they are targeted only to services at risk, and to specific users or group of users, where possible, and are issued by a judicial or independent administrative authority balancing all the rights at stake and assessing their necessity and proportionality.

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 proposal does not set requirements for specific service providers to withdraw from the EU.

The proposal relies on a thorough and publicly available impact assessment ⁽²⁾ and strives to achieve a fair balance in the protection of all fundamental rights impacted, including the right to privacy and the rights of the child enshrined in the Charter of Fundamental Rights of the European Union ⁽³⁾.

As is outlined in the Roadmap for lawful and effective access to data for law enforcement ⁽⁴⁾, the Commission recognises that encryption and other cybersecurity measures play an important role in protecting information systems from espionage and disruption and securing communications, privacy and personal data.

¹ <https://www.heise.de/news/Chefin-der-Signal-App-droht-mit-Rueckzug-aus-Europa-10688792.html>

⁽¹⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0209>.

⁽²⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022SC0209>.

⁽³⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

⁽⁴⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0349>.