

(English version)

**Question for written answer E-002044/25
to the Commission**

Catherine Griset (PFE), Christophe Bay (PFE), Mélanie Disdier (PFE), Julie Rechagneux (PFE), Séverine Werbrouck (PFE), Fabrice Leggeri (PFE), Gilles Pennelle (PFE), Pascale Piera (PFE)
(21 May 2025)

Subject: Message encryption

The Commission has begun to consider whether police forces could gain access to encrypted messages.

Although useful in the fight against organised crime, any backdoor could nevertheless be exploited by malicious actors, such as hackers, unscrupulous private companies or third country intelligence services.

As my colleague Aurélien Lopez-Liguori, Member of the French National Assembly, has noted, such backdoors would inevitably weaken encryption and therefore be a chink in the cybersecurity armour ⁽¹⁾.

The risk is such that a provision to that effect was rejected in a National Assembly debate a few weeks ago.

1. Will the Commission take that security risk into account before introducing any legislative proposals that require the various messaging services to contain a backdoor?
2. If necessary, will it ensure that any authorisation to override message encryption can only be issued by a judge, as part of a criminal investigation and for a limited period of time?
3. Finally, how does it intend to require messaging services owned (as almost all are) by non-EU companies to contain backdoors?

Supporter ⁽²⁾

Submitted: 21.5.2025

Answer given by Mr Brunner on behalf of the European Commission
(23 July 2025)

The Commission considers that the protection of fundamental rights, in particular privacy and data protection, and a strong cybersecurity are key elements of society.

In addition, encryption is one means of protecting confidentiality and is widely recognised as an essential tool for security and trust in open networks.

The communication on *ProtectEU: a European Internal Security Strategy* ⁽¹⁾, adopted on 1 April 2025, recalls those principles while stating that ensuring lawful access to data is key to investigate and take action against crime.

In response to the recommendations of the High-Level Group on Access to Data ⁽²⁾, the Commission will propose a Roadmap on Access to data with concrete measures to address the challenges faced by law enforcement to detect, prevent and investigate crime in the digital realm, including the abuse of emerging technologies to conceal their digital footprints.

On encryption more specifically, the Commission is setting up an expert group to prepare a Technology Roadmap on ensuring law enforcement authorities' lawful access to encrypted data.

Any possible solutions devised by the group shall be compatible with the applicable EU legal framework on fundamental rights, including privacy and data protection, and ensure a high level of cybersecurity.

¹ <https://lcp.fr/actualites/narcotrafic-l-assemblee-refuse-l-acces-aux-messageries-chiffrees-contre-l-avis-de-bruno>

² This question is supported by a Member other than the authors: Marie-Luce Brasier-Clain (PFE)

⁽¹⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148>.

⁽²⁾ https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en.