Law Enforcement Experts: Action against End-to-End Encryption Needed

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Thomas Wahl

European police chiefs called on industry and governments to take urgent action to ensure public safety on social media platforms. The privacy measures currently in place, such as end-to-end encryption, prevent technology companies from identifying and reporting all offences on their platforms. They will also prevent law enforcement agencies from obtaining this evidence and using it in investigations to prevent and prosecute the most serious offences, such as terrorism, child sexual abuse, human trafficking, drugs smuggling, murder, and economic crime. The industry must build in security by design in order to enable detection of harmful and illegal activities. The democratic governments must put in place frameworks that give law enforcement the information needed to keep publics safe, the Chiefs added.

The statement, supported by Europol, was published on 21 April 2024 - at the same day when Meta's Messenger platform rolled out end-to-end encryption.

AUTHOR

Thomas Wahl

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2024, Vol. 19(1) eucrim
ISSN: 1862-6947
https://eucrim.eu

The statement by the European police chiefs came amid further requests from the part of law enforcement agencies to torpedo the introduction of stronger end-to-end encryption by tech companies. On 21 May 2024, the High-Level Group (HLG) on Access to Data for Effective Law Enforcement adopted 42 recommendations for the further development of Union policies and legislation to enhance and improve law enforcement access to data. The recommendations, *inter alia*, call for the re-introduction of mass telecommunications surveillance ("data retention") and the undermining of encrypted communication systems.

In July 2024, media leaked a "non-paper" that was produced by the Swedish government and circulated in the Council stating that "a fundamental change in perspective" in the fight against terrorism and organised crime is needed, because too many proposals are "watered down" by fundamental rights considerations. The Swedish government proposed a four-pronged approach involving the establishment of "adequate EU institutional working methods"; "Follow the money"; "Going Dark – Access to digital data"; and "Making the most of operational support."

NGOs and some MEPs raised eyebrows at the push from the law enforcement side. Even though no formal proposals have been made yet, they criticised the suggestions to be an "excessive leap directly into a fully monitored society."

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union