New Report on Encryption by EU Innovation Hub

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle
Deputy Head of Section
Academy of European Law

Published in
2024, Vol. 19(2) eucrim
ISSN: 1862-6947
https://eucrim.eu

At the beginning of June 2024, the EU Innovation Hub for Internal Security published its first Report on Encryption. The report analyses the topic of encryption from legislative, technical, and developmental points of view.

Against the background of the ever-increasing presence of encrypted data in criminal investigations, access to such information by law enforcement authorities has been the subject of a long-standing discussion about how the privacy rights of individuals and collective security must be balanced: how can lawful interception coexist with encryption without undermining cybersecurity and/or privacy?

According to the report, a framework to access encrypted communications is steadily taking shape in the EU. Although the newly adopted e-evidence package (→ eucrim 2/2023, 165-168) is a step in the right direction, namely towards enhancing law enforcement access to electronic evidence, many questions remain concerning the admissibility of evidence gathered from encrypted communication channels and the challenges arising from various technologies. Next to the national, European, and international legislation on encryption, the report also looks at encryption challenges and opportunities in relation to, for instance, quantum computing, cryptocurrencies, biometric data, the Domain Name System (DNS), telecommunication technologies, artificial intelligence (AI), and large language models (LLMs). The report draws the following conclusions:

- Some EU Member States have recently made amendments to existing national legislation in areas relevant for bypassing encryption. Extended search capabilities and means for targeted lawful access could be beneficial in capturing encrypted data.
- Differences in data retention periods between the EU Member States (which the report estimates as problematically short in some cases) might be slightly outbalanced by the possibilities to transmit requested data faster under the new EU e-evidence package.
- A wider debate on the introduction/use of alternative means of bypassing encryption (e.g. client-side scanning) is necessary.
- The problems created by home routing in 4G and 5G networks (individuals within national borders that use a foreign SIM card cannot be intercepted unless the foreign service provider cooperates with the domestic provider), may – for the moment – require that privacy-enhancing technologies be disabled in home routing.
- Interception technologies for user identification should be a legal requirement for the next generation of mobile networks (5G and 6G).
- From a technical perspective, there is a need for further research to reach a solution where both individual privacy and lawful interception are respected.

- In order to identify criminals using cryptocurrencies, collaboration with academia and private industry is needed, so that technological trends can be monitored and novel tools can be created.
- There is a need for DNS encryption, which, if implemented, would allow law enforcement to access and process suspects' DNS traffic.
- The need exists for a legal framework on the use of artificial intelligence and large language models, underpinned by robust and adequate data protection safeguards, in which law enforcement authorities can leverage the same modern technologies as other stakeholders in the private sector and academia.
- Quantum computing can significantly improve the investigative capabilities of law enforcement.
- Ultimately, relevant stakeholders in the JHA domain must be made aware of these developments and be provided with the means to stay on top of these technological advancements.

The encryption report was produced by the following members of the EU Innovation Hub for Internal Security: Europol, Eurojust, the European Commission's Directorate-General for Migration and Home Affairs (DG HOME), the European Commission's Joint Research Center (JRC), the European Council's Counter-Terrorism Coordinator, and the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA). Hosted at Europol, the Hub is a network that works on innovative tools and effective solutions to support internal security actors in the EU and its Member States. The Hub team is composed of staff from different EU Agencies and Member States. Work on encryption/decryption technologies is one of the Hub's top priorities.

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