Council of the
European Union

Brussels, 18 September 2020
(OR. en)

10730/20

LIMITE

COSI 133
ENFOPOL 215
CYBER 158
DATAPROTECT 84
IXIM 91
COPEN 248
JAI 708

NOTE

From:	Commission services
To:	Delegations
Subject:	End-to-end encryption in criminal investigations and prosecution

Delegations will find attached a note from Commission services on the "End-to-end encryption in criminal investigations and prosecution".

EUROPEAN COMMISSION

End-to-end encryption in criminal investigations and prosecution

Note from the Commission services[1]

1. Introduction

Encryption is an important tool for the protection of cybersecurity and fundamental rights, such as privacy, including the confidentiality of communications, and personal data[2]. Inter alia, it may safeguard international data transfers[3]. At the same time, it can also be used as a secure channel for perpetrators where they can hide their actions from law enforcement and the judiciary.

---

1 This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and does contain confidential and/or privileged material.

2 Existing European Union legislation specifically refers to the use of encryption as a possible measure to ensure an appropriate level of security for the protection of the fundamental rights and strengthening cybersecurity: Article 32(1a), 34(3a), 6(4e), recital (83) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; recital (60), article 31(3a) of the Law Enforcement Directive; recital (20) in conjunction with article 4 of the ePrivacy Directive 2002/58/EC; recital (40) of Regulation (EU) 2019/881 (Cybersecurity Act).

3 EDPB letter, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-mep-moritz-korner-regarding-relevance-encryption_en

The application of encryption in technology has become readily accessible, often free of charge, as industry is opting to include encryption features by default in their products. Criminals can make use of readily available, off-the-shelf solutions conceived for legitimate purposes. This makes the work of law enforcement and the judiciary more challenging, as they seek to obtain lawful access to evidence. During a workshop with experts[4], law enforcement and the judiciary noted that the use of encryption has impacted the ability to gain lawful access to electronic evidence in between 25 and 100% of their cases – depending on the crime area. They estimated that the use for criminal purposes of legitimate end-to-end encrypted technology in online communications platforms will continue to increase.

The recent dismantling of the EncroChat network in a joint investigation coordinated by Eurojust and Europol shows the degree to which those involved in criminal activity utilise all available technology, such as crypto telephones, which go well beyond publicly available end-to-end encrypted services. Gaining lawful access to these especially designed, encrypted phone networks used by criminals involved in the planning and execution of violent attacks, corruption, attempted murders and large-scale drug trafficking, among others, led to more than 800 arrests in this Europe-wide operation.[5] Successful operations of this kind remain the exception at the moment, due in part to limitations in technical capabilities available to law enforcement, and also because the existing legal landscape across EU Member States is very diverse. Few Member States have specific legal provisions allowing law enforcement and judicial authorities to tackle encryption[6].

---

4 High-level stakeholder dialogue on encryption with prosecutors. Held with the European Judicial Cybercrime Network (EJCN) at Eurojust on 13th November 2019.

5 https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

6 More detailed information national legal regimes can be found in the second observatory report on encryption prepared jointly by Europol and Eurojust, https://www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption.

Member States have discussed the challenges of encryption and called to find solutions that allow law enforcement and other competent authorities to gain lawful access to digital evidence, without prohibiting or generally weakening encryption, and in full respect of privacy and fair trial guarantees consistent with applicable law.[7]

The Commission has proposed six practical measures[8] to support law enforcement and the judiciary when they encounter encryption in criminal investigations. The focus of these measures has been on data "at rest", that is, encrypted devices and hard drives. However, they also included informal discussions on end-to-end encryption with experts from law enforcement and the judiciary, academia, non-governmental organisations (NGOs), over-the-top-service providers (OTTs), telecommunication providers, and the security industry. Participants:

- agreed on the importance of encryption as a tool to protect cybersecurity and fundamental rights;

- law enforcement and prosecutors confirmed that the issues posed by encryption in criminal investigations and prosecutions will continue to increase, as encryption use becomes more widespread. They pointed out the need to have access to a range of measures, including the right tools and capabilities deployable in full respect of fundamental rights and legal safeguards, together with the necessary training;

- OTTs confirmed the importance of setting out collaborative channels targeting more constructive communication with law enforcement that facilitates structural and technical assistance and educates law enforcement on the type of assistance companies can provide.

---

7 The issue of encryption was discussed during the Justice and Home Affairs (JHA) Council meeting of December 2016 http://data.consilium.europa.eu/doc/document/ST-15391-2016-INIT/en/pdf, followed by the European Council conclusions on security and defence adopted in June 2017 https://www.consilium.europa.eu/en/press/press-releases/2017/06/22/euco-security-defence/. Most recently, the Justice and Home Affairs Council Conclusions on on combating the sexual abuse of children in October 2019 raised the point, https://data.consilium.europa.eu/doc/document/ST-12862-2019-INIT/en/pdf.

8 Eleventh progress report towards an effective and genuine Security Union, COM/2017/608 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1512558067781&uri=CELEX:52017DC0608.

A reflection is ongoing on possible technical solutions to detect and report child sexual abuse in end-to-end encrypted electronic communications, and to address regulatory and operational challenges and opportunities in the fight against these crimes[9].

A number of third countries have also highlighted the issue of access by law enforcement authorities to encrypted material. Australia, Canada, New Zealand, the United Kingdom and the United States issued a joint statement in 2019 calling on technology companies to consider in the design of their encrypted products and services possibilities for governments, acting with appropriate legal authority, to obtain access to data in a readable and usable format. They also called on industry to engage with them in a joint quest for lawful, proportionate solutions.[10] Some third countries have started implementing their own national solutions.[11]

On the other hand, weakening any part of an encrypted system could lead to weakening the system as a whole[12] with detrimental effects on fundamental rights, including the rights to privacy and protection of personal data. Encryption can indeed ensure a more effective exercise and protection of such rights (e.g. freedom of expression and opinion, data protection), and security of international data transfers.

---

9 In light of the Commission's adoption of the Strategy on a more effective fight against child sexual abuse (COM 2020 (607)final), an expert process has been launched under the EU Internet Forum with industry, to map and preliminarily assess, by the end of 2020, possible technical solutions to detect and report child sexual abuse in end-to-end encrypted electronic communications. The same work strand will also address the specific regulatory and operational challenges and opportunities in the fight against these crimes to complement the efforts related to encryption more generally.

10 https://www.reuters.com/article/us-security-fiveeyes-britain/five-eyes-security-alliance-calls-for-access-to-encrypted-material-idUSKCN1UP199.

11 For example, Australia adopted an Assistance and Access Act in 2018, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption.

12 IEEE https://globalpolicy.ieee.org/new-ieee-position-statement-supports-strong-encryption-for-confidentiality-and-data-integrity/; The German Federal Data Protection Authority's Statement on a right to encryption in the context of the hearing organised by the German Federal Parliament; Article 29 Working Party statement on encryption of 13 April 2018 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229; ENISA Opinion Paper on encryption of 2016, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption.

2. Moving forward

Based on the expert process, key considerations are set out below to support the reflection in the Council, to facilitate and inform the identification of solutions for targeted lawful access by law enforcement and judiciary authorities to information in end-to-end encrypted communications, while ensuring that privacy and data protection is respected.

- Orders to access encrypted electronic communication must be targeted to specific individuals or groups of individuals in the context of the investigation of a specific crime, and be proportionate. They must be issued or be subject to prior validation by a judiciary authority. Transparent reporting procedures, as well as appropriate review and redress mechanisms are necessary.

- Technical solutions constituting a weakening or directly or indirectly banning of encryption will not be supported.

- Technical solutions to access encrypted information should be used only where necessary, i.e. where they are effective and where other, less intrusive measures are not available. They must be proportionate, used in a targeted and in the least intrusive way.

- Transmission of data to law enforcement authorities should benefit from state-of-the-art security measures to comply with data protection rules.

- Given the broad spectrum of encryption solutions that may be concurrently deployed on devices or systems to provide multiple layers of protection, in the opinion of the Commission services there should be no single prescribed technical solution to provide access to the encrypted data (principle of technological neutrality). Companies providing the encryption for their products can contribute to identifying the best solutions.

- Industry, civil society and academia support, as well as independent expert advice such as by EU bodies mandated to provide cybersecurity and data protection expertise, is indispensable.

This note of the Commission services is submitted to Council to stimulate debate. Member States may wish:

- *To comment on the above key considerations as a means of finding a common ground upon which the debate on encryption may progress further, and*

- *To provide their comments on what they consider to be the appropriate next steps.*