Council of the European Union

Brussels, 16 November 2020
(OR. en)

12864/20

LIMITE

JAI 974
COSI 206
CATS 87
ENFOPOL 304
COPEN 323
DATAPROTECT 127
CYBER 232
IXIM 115

NOTE

From:	Presidency
To:	Delegations
Subject:	Recommendations for a way forward on the topic of encryption

Protecting the privacy of communications and other fundamental rights through encryption on the one hand and upholding the investigation powers of law enforcement in the digital world on the other hand are extremely important. Any actions to gain lawful access must balance these interests carefully. MS play a crucial role in this. From the point of view of the Presidency the following should be considered in order to provide a structured follow up to this topic, further to the Council Resolution on encryption[1], presented for endorsement to COSI on 19 November 2020:

1. We continue to support strong encryption. Encryption is an anchor of confidence in digitalisation and protection of fundamental rights and should be promoted and developed. At the same time, it is important to acknowledge that the use and abuse of the digital environment by criminals means that the various tools that have been created to ensure the privacy of communication and data of the citizens are being increasingly used for criminal purposes. It is our responsibility, together, to find balance between these important public interests.

[1] 12863/20

2. We are determined to balance carefully the interests of protecting privacy, fundamental rights and security of communications through encryption but at the same time upholding the ability for competent authorities in the area of security and criminal justice to lawfully access relevant data for legitimate, clearly defined purposes in fighting serious and/or organized crime and terrorism, including in the digital world.

3. We acknowledge this dilemma and are determined to find ways that will not compromise either one, upholding the principle of security through encryption and security despite encryption. Various technical options should be identified and evaluated for this purpose.

4. We would like to call on all Member States, the Commission and the other EU institutions and agencies to combine efforts to jointly develop technical and operational solutions built on the principles of legality, necessity and proportionality in close consultation with service providers and the relevant authorities.

5. We aim for a coordinated, consistent EU position on the topic of encryption because we have a joint challenge concerning encrypted data in the field of fighting terrorism, organized crime, child sexual abuse, etc. At the same time, we must value encryption as an important technology for the digital life of today and the protection of fundamental rights. We need to agree upon these complex issues and improve coordination at EU level.

6. We are determined to maintain a close exchange with the initiators of the “International Statement: End-to-End Encryption and Public Safety” (UK, USA, Australia, New Zealand, Canada, India, Japan) and other relevant international actors in order to balance the different interests carefully. We need to establish and keep an ongoing dialogue especially with the UK in that matter.

7. We would like to combine forces and build up a lasting dialogue between Member States, the technology industry, civil society and academia with regard to encryption. The EU Innovation Hub at Europol and national research and development teams play an important role as partners for the technology industry to keep up the cooperation and dialogue with the technology industry, academia and stakeholders in the Member States.

8. We acknowledge internet service providers and social media platforms as important stakeholders in the discussion and are determined to include them in the discussion in order to lift the technical expertise to the next level and stimulate the dialogue.

9. We are convinced of the importance of a continued assessment of the appropriate technical, operational and legal solutions and aspects especially given the constant development in encryption techniques.

10. We emphasize the need for high-quality training programs for officers working on cases in the Member States to elevate the level of expertise to match that of the criminal environment. We aim to enable agencies in the Member States to be adequately familiar with the underlying technology and therefore calls on qualified European agencies and/or agencies in the Member States to step in and contribute to standardized training programs.

11. We call upon Member States and EU Institutions to actively take part in technical standardisation processes, particularly at the Internet Engineering Task Force (IETF) in order to give a voice to the views of Member State agencies in current and future technical developments.

12. We acknowledge the need to review the effects arising from different relevant regulatory frameworks in order to develop further a consistent regulatory framework across the EU that would allow competent authorities to carry out their operational tasks. We underline that the EU can leverage the strength of its single market to ensure that device manufacturers and service providers create technologies that meet the Member States' needs while preserving the benefits of encryption.

COSI is invited to express its views on the next steps and indicate other aspects that might need to be considered for providing a follow up.