High-Level Group
on Access to Data for Effective Law Enforcement

Working Group 3 – Real time access to communication data

13 February 2024, Brussels

Agenda

1. Arrival, coffee and registration	**09:30-10:00**
2. Introduction - *Welcome by the chair, European Commission* - *Brief review of the First Meeting of Working Group 3 and of the Second Plenary of the HLEG: identified issues and areas for action* - *Tour de table*	**10:00-10:30**
3. Exploring the conditions for lawful interception of Electronic Communication Providers. *This session will explore the conditions and options for lawful interception of communication data, focusing on the specific use case OTTs. The group will seek to identify and agree on a set of common principles.* *It will be introduced by invited speakers:* • *Microsoft on the perspective of OTTs* • *Netherlands Public Prosecutors Office on the perspective of the judiciary* • *Head of National Technical&Tactical Support Unit, BE Federal Police* • *Commission on the interplay with e-evidence and other cooperation instruments*	**10:30-12:30**
	12:30-13:30

Lunch break

4. Targeted lawful remote access to devices

This session will explore conditions for legal certainty when using special technics to access data on devices remotely, based on feed-back from Encrochat & Sky ECC.

From a technical perspective, the group will also explore conditions for an EU industrial approach to lawful remote access.

13:30-15:00

Speakers:

- *French Vice-procureur and Belgian Prosecutor on EncroChat/Sky ECC challenges*
- *Vice Questore della Polizia di Stato on admissibility of evidence from the receiving state's perspective*
- *Commission/JRC on vulnerability management*

Coffee break **15:00-15.30**

5. Challenges pertaining to encryption of content data

This session will explore measures to better assess the impact and mitigate challenges posed by encryption.

i) When encrypted services (e.g. end-to-end encryption) are implemented by non-traditional CSPs.

ii) When encrypted services such as RCS (Rich Communication Services) or voice calls for inbound roamers, are implemented by traditional CSPs.

In a more forward-looking perspective, the group will also explore the legal and technical viability of policy approaches to develop communication technologies (e.g. 6G) which are secured by default while allowing exceptional lawful access by design **15.30-16.30**

Speakers:

- *SE police senior legal advisor on making use of Law Enforcement Operational Requirements (LEON)*
- *Vice-chair of ETSI TC Cyber & Convenor of CEN/CENELEC JTC13 WG1 on cybersecurity and data protection) on lawful access vs strong cybersecurity*
- *Europol on risks to LI pertaining to "home-routing".*

6. Conclusion and next steps **16.30-16.50**

7. Any Other Business **16.50-17.00**