EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS

Directorate D – Internal Security

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

Report of the Public Consultation Meeting 20th February 2024

1. BACKGROUND

The public consultation meeting of the High-Level Group (HLG) on Access to Data for Effective Law Enforcement took place in an online format on 20 February 2024, and was chaired by the European Commission. The meeting counted 187 external participants representing, *inter alia*, Academia, Civil Society, Industry, and Law Enforcement, who were all invited to set out their positions on important issues for current and future legal and policy frameworks for law enforcement access to data as well as on solutions suggested by the members of the working groups.

This document provides a non-exhaustive summary of the interventions made by participants at the public consultation during the meeting. It reflects exclusively the views of the participants and does not represent an official position of the European Commission or the Council.

2. INTRODUCTORY REMARKS

In their welcoming words, the Chairs reflected on the creation of the HLG, with the mandate originally granted under the Swedish Presidency of the Council and subsequently carried forward by the Spanish and Belgian Presidencies respectively.

A representative of the former Swedish Presidency, under whose guidance the group had originally been set up, further added to the introductory comments delivered by the European Commission and set out 3 key clarifications which were considered instrumental prior to the discussions of the day, these being: why the work of the HLG was necessary; the various interests that needed to be considered; and the long term objectives of the group as a whole.

In the discussions that followed the introductory remarks, Civil Society representatives highlighted that there should be no attempt on behalf of the recommendations and initiatives that will be derived from the work of the HLG to redefine fundamental rights. They also recalled the repeated assertions of industry that a so-called law enforcement 'front door' for accessing data has been deemed technically impossible. They also set out that they were, as a whole, concerned with the lack of transparency regarding the work of the HLG.

3. ACCESS TO DATA AT REST IN A USER'S DEVICE (WORKING GROUP 1)

In the discussions, the following points related to the work and outputs of Working Group 1, dedicated to discussing access to data at rest in a user's device, were raised:

- Industry representative highlighted the existence of existing groups of experts, namely the Europol Data Protection Experts network (EDEN), and that work efforts of the HLG should not be duplicated.

- Civil society representatives stated that the narrow view of Working Group 1 of the HLG was of concern, as their assessment was that it does not aptly consider fundamental rights concerns related to setting out lawful access pathways to these devices. In addition, these representatives did not consider that compromising security of all in order to be able to conduct criminal investigations was a positive trade-off, especially in the absence of statistics to support law enforcement claims that accessing data at rest in user's devices is proving increasingly more difficult. In addition, they considered that the Encrochat involved bulk collection and that there were no individualised suspicions as there was access to all communications. They considered that individuals should only be targeted on the basis of suspicion, and the amount of data should be limited solely to the minimum volume necessary.

- Representatives from Civil Society also indicated that the cost of finding and exploiting vulnerabilities in order to be able to access data constituted an incentive for investigatory authorities to define their targets, the volume of data required, and use these techniques in moderation, and were therefore a preferable option as opposed to general lawful access subject to safeguards.

4. ACCESS TO DATA AT REST IN A SERVICE PROVIDER'S SYSTEM (WORKING GROUP 2)

In the discussions, the following points related to the work and outputs of Working Group 2, dedicated to discussing access to data at rest in a service provider's system, were raised:

- Civil Society representatives noted that the work of Working Group 2 on data retention has potentially significant implications for fundamental rights, and that a number of national legislations currently in place are in breach of relevant Court rulings. They asserted that Member States who have tried to implement the requirements of the CJEU still do not meet proportionality requirements, and the perceived need to launch infringement proceedings. Recommendations from Working Group 2 should seek the repealing of current data retention laws in Member States.

- Civil society representatives also questioned the capacity of data retention schemes to be enforceable for Over-The-Top Service providers (OTTs) who are based outside of the EU, and also raised that imposing obligations on them to retain data which they do not currently have or retain would not constitute a positive development, as it goes against the principle of data minimisation, and could risk these services leaving the EU market.

- Lastly, representatives from Civil Society questioned the supposed necessity of any data retention legislation for law enforcement and stressed that, given the huge amount of data available nowadays, the need to avoid data retention to limit any impact on users was even bigger than ten years ago.

- Representatives from Academia noted the existence of disparate practices across Member States related to data retention and referred to the necessity of creating a common EU framework. The representatives highlighted that safeguards and guarantees could be defined at the access level (as opposed to focusing solely on the retention stage) and referred to the legislation on financial intelligence by means of example. However, this was challenged by Civil Society representatives, who set out that safeguards at the access level remained unacceptable given the degree of interference with fundamental rights that stems from data retention.

- Industry representatives highlighted that, regarding the implementation of any harmonised EU framework for data retention, the high costs of retaining data, potential liability of service providers and lack of regulation on cost-sharing between providers/customers/authorities must also be considered. However, it was also indicated that certain industry actors would welcome a pan-European framework for retention in line with CJEU case-law, as long as this would not require further retention of data than that generated in the course of business.

5. REAL TIME ACCESS TO DATA IN TRANSIT (WORKING GROUP 3)

In the discussions, the following points related to the work and outputs of Working Group 3, dedicated to discussing access to real time data in transit, were raised:

- Industry representatives put forth that some private sector entities do the utmost to respond to law enforcement requests for data, but that in relation to access to data in transit there must be safeguards in the form of judicial oversight to any interception order, and that any such order must be targeted, have a limited scope, confer no direct access rights, and lead to no weakening of encryption.

- Civil Society representatives highlighted the issues that are caused by the lack of an EU definition on serious crime, and stated that no oversight mechanism could accommodate the intrusion on privacy of the introduction of backdoors.

- Academia representatives also questioned how data in transit could be legally defined in a digital environment, highlighting that in some Member States the distinction between data in transit and data at rest in a provider's system has already been abolished.

6. RESPONSES

To respond to the issues raised over the course of the day's discussions, participants of the Public Consultation meeting, *inter alia*, suggested:

- Close cooperation between all entities and actors working on matters related to law enforcement access to data, including relevant expert groups attached to EUROPOL, EUROJUST, or data protection authorities;

- Consideration of negotiation of agreements on cost sharing (including between providers and customers) for infrastructure required to perform (large scale) data retention by service providers (including OTTs);

- Common EU framework on data retention in line with the case-law of the CJEU;

- Collection of comprehensive data on law enforcement practices concerning access to data as a basis for evidence-based policy making;

- Strengthening of safeguards around law enforcement access to data, including as regards the discharging of proportionality requirements and accountability, in addition to safeguards concerning data retention;

- Facilitation of a common understanding of terminology in the context of law enforcement access to data.