Background document

Possible Avenues to Explore Regarding the Challenges Faced by Law Enforcement Related to Access to Data

Input to the third plenary meeting of the High-Level Group on access to data for effective law enforcement

1 March 2024

1. Introduction

The High-Level Group on access to data for effective law enforcement (HLG), launched by the Commission and the Swedish Presidency in June 2023, and co-chaired by the Commission and the rotating Presidency of the Council of the EU, explores challenges that law enforcement practitioners in the Union face in their daily work in connection to access to data and potential solutions to overcome them, with the aim of ensuring the availability of effective law enforcement tools to fight crime and enhance public security in the digital age, in full respect of fundamental rights.

Digitally generated, processed, or stored communication data (both metadata and content data) is an increasingly important component of modern criminal investigations. However, law enforcement authorities face increasing operational challenges when seeking to lawfully access data digitally generated, processed, or stored in a readable format, be it (i) data at rest in a user's device, (ii) data at rest in a provider's system, or (iii) data in transit.

Access to this data is understood as access granted to law enforcement subject to judicial authorisation when required, in the context of criminal investigations and on a case-by-case basis. As a rule, in the cases where such judicial authorisation is required, it represents an integral part of the applicable legal and operational framework for access to this data by law enforcement, whilst ensuring that such access is granted where necessary and in full application of criminal procedural safeguards. Access to data on behalf of law enforcement authorities has to be achieved in compliance with data protection, privacy, and cybersecurity legislation, as well as the Court of Justice of the European Union (CJEU) case-law on these matters and applicable standards on procedural safeguards.

The three Working Groups established under the HLG started their work by taking stock of the current situation and focusing on identifying and prioritising the main challenges encountered by law enforcement, and the drivers that underpin them, and subsequently reported back to the second plenary meeting of the HLG in November 2023.

At the second plenary meeting, delegates were presented with a document outlining the summary of the challenges identified by members across the first round of meetings the three Working Groups to facilitate discussions, and subsequently frame the context in which the discussions in the second round of Working Group meetings would take place. Based on these discussions, 3 key areas were identified to explore potential solutions: **capacity building, legislative (including soft law),** and **industry cooperation/standardisation.**

In addition to the meetings of the three working groups, on 20 February 2024 a **Public Consultation meeting** was organised during which civil society stakeholders, industry representatives, and academia were 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 and their own proposals in this respect. The attendees of the Public Consultation meeting highlighted several challenges for consideration:

1) Compliance of national data retention regimes with the Court of Justice case-law;
2) High costs of retaining data, potential liability of service providers and lack of regulation on cost-sharing between providers/customers/authorities;
3) Lack of evidence supporting the needs reported by law enforcement;
4) (Risk of) circumvention of proportionality rules and procedural rights and safeguards, including legal professional privileges;
5) Conflicts of law faced by service providers due to differences in national legal regimes on access to data;
6) Risk to security of services and data through attempts to establish access to encryption or direct access channels to Over-The-Top service providers' (OTTs) services/data.

To respond to these challenges, participants of the Public Consultation meeting, inter alia, suggested:

1) 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;
2) 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);
3) Common EU framework on data retention in line with the case-law of the CJEU;
4) Collection of comprehensive data on law enforcement practices concerning access to data as a basis for evidence-based policy making;
5) 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;
6) Facilitation of a common understanding of terminology in the context of law enforcement access to data.

A more comprehensive report on the Public Consultation meeting, including concerns that were raised and avenues for possible ways forward regarding the HLG, is to be made public.

While the expert working groups have focused on the issues from a vertical perspective as per the scope of their allocated data type, this plenary marks the start of the recommendation stage of the HLG and therefore is an astute time to horizontalize potential recommendations across different solution areas as opposed to viewing them solely through the lenses of each individual group. This approach also ensures that the potential recommendations do not overlap and enables an exploration of the relationship and interaction between the various measures.

This background document provides a non-exhaustive summary what these avenues of solutions could consist of, as identified across the three Working Groups by the experts, in a horizontal structure as per the 3 key solution areas. The below summary reflects exclusively the views of the experts and does not represent an official position of the European Commission or the Council.

2. Suggested solutions

Each of the individual Working Groups were tasked with identifying potential solutions to the issues that law enforcement face regarding access to, respectively, (i) data at rest in a user's device, (ii) data at rest in a provider's system, or (iii) data in transit, with these solutions being categorised under **capacity building, legislative,** or building on **industry cooperation/standardisation.**

2.1. Capacity Building

Group	Suggested solutions
Working Group 1	• Upscale and better coordinate research and development for digital forensic tools at the EU level, including by fostering collaborative developments, partnerships with industry, as well as the sharing of such tools and expertise among the Member States' digital forensics departments. • Set mechanisms, (e.g., an EU certification scheme on digital forensics, train the trainer programs, reinforcement of the CEPOL Cyber academy) and allocate appropriate funding to provide EU law enforcement with adequate digital forensic skills. • Maintain and improve existing networks which foster cooperation between Member State digital forensic departments as well as with Europol, including raising awareness of these networks for practitioners that conduct investigations. • Establish a harmonised certification system for digital forensic tools, processes, and competencies to ensure compliance with accountability and forensic standards within the Union.
Working Group 2	• Foster the development of Member States' capacities to access, exchange, and process digital evidence, notably to address the challenges of large volume datasets. • Support projects and mechanisms providing law enforcement and judicial authorities with the necessary knowledge to effectively request access to data (e.g., SIRIUS).
Working Group 3	• Ensure that relevant capacities exist to implement real-time interception of Electronic Communication Services (from process, network capacity, and data format perspectives) including when requested through international cooperation instruments. • Foster the development of a trusted environment for the development, acquisition, and use of intrusive live intercept capabilities, in compliance with fundamental rights (for example by setting a framework for vulnerability disclosure or for the certification/auditability of solutions).

2.2. **Legislative**

Group	Suggested solutions
Working Group 1	• Legislation for tackling the use of encryption devices which have been proven to be solely used for the purpose of communication between criminal actors. • Set obligations for technology providers to facilitate access to data at rest in user's devices when requested by judicial authorities, for example by providing technical assistance.
Working Group 2	• Harmonisation across the EU of rules and safeguards regarding data availability, retention, and access. • Enforcement of a level playing field for all communication service providers, including OTTs, on retention requirements.
Working Group 3	• Enforcement of a level playing field for all communication service providers, including OTTs, on lawful interception requirements. • Clarify and seek to harmonise legislation regarding the location of users, service providers, and servers to provide legal certainty for both the requester and requestee when executing a lawful intercept request. • Set out a framework to determine what constitutes a rogue communication service provider (i.e., a communication service provider that refuses to comply with legal obligations). • Legislation to sanction or block communication service providers that are not compliant with EU laws. • On Home-routing challenges for lawful interception (difficulty in intercepting 4G/5G communications for users with a foreign SIM card): define and enforce best practices for Communication Service Providers that maintain lawful interception capability as well as security of communications.

2.3. **Industry cooperation / Standardisation**

Group	Suggested solutions
Working Group 1	• Increase and coordinate the EU effort to engage with identified relevant standardisation bodies. • Increase and codify cooperation between commercial companies and law enforcement agencies such that technical product documentation and source code are shared voluntarily. • Handbook outlining how to engage with industry to gain insight into the legal processes to gain access to data stored in users' devices.
Working Group 2	• Clarify the criteria and obligations for OTTs on the types of data they collect and retain.

	• Agree on mechanisms for robust cooperation with communication and technology providers (e.g., to increase transparency and better address technological shifts). • Develop standardised and secured channels for exchanges with service providers via the e-evidence exchange system. • Foster Member States' involvement in setting up standardised formats for data retention and access, based on ETSI standards (notably for categories of data currently not covered by standards).
Working Group 3	• Ensure that the Law Enforcement Operational Needs (LEON) on lawful interception be considered, where appropriate, for future developments on standardisation, cooperation with industry and possible Member State and/or EU legislation. • Seek to develop EU standards that are needed to develop secured communication technologies compliant with lawful access and data protection requirements. • Foster the identification and further development of certification frameworks that guarantees the conformity of lawful access mechanisms with requirements (e.g., on auditability, transparency, and accountability).

3. **Questions**

Based on the possible solutions that transpired from the discussions, the following questions have been prepared for discussion during the third plenary meeting:

1. *Does the Plenary agree with and/or consider the suggested solutions that have been addressed in the table appropriate?*

2. *Are there any further solutions or combinations of solutions that should be addressed?*

3. *With some suggested solutions set out, what are possible concrete recommendations for the way forward that the respective Working Groups should explore in their third meetings? Please consider whether any such recommendations would best fit under capacity building, legislative, or industry cooperation/standardisation or a combination thereof.*

4. *Within this context, what are possible recommendations on related measures to be taken to support particular solutions, for instance, as regards data collection needs for evidence-based policy making?*