Working Group 2, Access to Data at Rest in a Provider's System

Request for input from experts

To date, two meetings of the Working Group 2 of the High-level Group (HLG) on access to data for effective law enforcement, focused on Access to Data at Rest in a Provider's System have taken place, on 6 September 2023 and on 16 January 2024 respectively. The first meeting focused on identifying existing challenges and gaps in law enforcement capacity to lawfully access data, while the second discussed more in-depth potential solutions to those challenges.

The third meeting on 19 March will allow the experts to agree on recommendations to address the identified challenges and drivers/legal constraints. Such recommendations will be then presented at the next Plenary meeting on 17 May.

To this end, experts are kindly requested to provide at least one recommendation for each of the solution areas that are being explored (legislative perspectives, capacity building, standardisation/cooperation with industry). The overall contribution should consist of a maximum of 2 pages of potential recommendations.

For ease of reference, the section below provides a summary of the main topics that have emerged during previous discussions, and a table summarising the identified problems and potential solutions. Experts will also find in Annex the background document circulated in view of the last Plenary session of 1 March 2024. In addition, experts will find the presentations delivered during the meetings of the working group in the Workspace for the experts of the HLG.

SUMMARY OF PREVIOUS MEETINGS

WG2 met for the first time in September 2023. In that meeting, based on typical case scenarios showcasing success stories and failures to overcome certain obstacles and challenges related to access to data, the experts identified challenges and capacity gaps that law enforcement authorities face regarding access to data at rest in a provider's system.

Experts shared a general common understanding of the **need for data retention**. Despite the fact that digital data is not the only evidence required to solve any given case, several experts stressed that it is needed or of relevance in almost all investigations, due to the overall digitalisation of our society. Retaining data to enable subsequent LEA access is therefore of fundamental importance for effective law enforcement.

Many experts expressed the view that there are no viable alternatives to attain the same objective, nor are there less intrusive alternatives to data retention. As means of example, some experts referred to NCMEC cases: in the absence of data retention that allows access to data, LEAs need to use more intrusive measures and, on occasion, the re-victimisation of victims occurs. Other experts emphasized how access to data can be useful to law enforcement authorities' investigations not only in terms of the role it can play in potentially , but also for preventing further crimes from being committed .

Lack of legal certainty and harmonised rules and safeguards on data retention was described as a significant problem for LEAs when carrying out investigations, for service providers when having to respond to requests from a MS with different retention rules. Many experts called for a harmonised EU solution on data retention, while others also showed opposition to such an initiative.

While acknowledging the call from EU institutions (European Court of Justice, European Parliament) and other stakeholders alike for **hard data** showing the impact of a lack of data retention legislation at EU level, practitioners, highlighted that the need to retain data in order to fight crime is not necessarily quantifiable in terms of statistics or categorisation of data, thus they had not been in a position to collect such an evidence so far.

Some experts also highlighted the difficulty of specifying types of crime requiring data retention; rather, they suggested to differentiate between data retention and access to data.

Experts strongly shared the view that any solution to the current challenges needs to be **technology-neutral**, in order to cover any future technical developments. Emphasis was put on the need for such solutions to create obligations for **all service providers**, including OTTs, who should be compelled to reply to requests from LEAs and be transparent with regard to the data that they collect for business purposes.

Related to this, many participants highlighted that for any solution to be viable, cooperation with industry is needed. **Standardisation** was indicated as a possible solution that needs to be further analysed and which could let providers understand the type of response they need to provide in the most integrated and cost-efficient way for both service providers and national authorities. Some experts stressed that requests by LEAs to providers generate costs for them, and that this aspect should also be taken into account.

Based on these discussions, in the following meeting of the WG, on 16 January 2024, experts structured the discussions on possible solutions along three strands: i) legislative solutions; ii) capacity building iii) cooperation with industry.

1. Legislative solutions

After having been provided with an overview on the history of data retention and data access at EU level, the experts discussed the requirements set by the Court of Justice of the EU (CJEU) and noted the evolution of the Court's thinking. In particular, they showed interest in the pending Hadopi case, in which the AG Szpunar invited the Court to adopt 'a more pragmatic approach'.

> Law enforcement and telecommunication providers representatives from MSs whose legal systems they consider to fulfil the requirements of the Court, presented the manner in which their legislation functions (how targeted retention based on geographic areas and categories of persons is applied in their territories). The presentations showed some of the complexities of implementing these criteria (i.e. adapting technology such as cell coverage to the requirements of the law, cases of persons travelling between different retention zones, "targeting" resulting in covering the majority of the territory, risks of legal challenges on the basis of systemic bias and discrimination). Also, one expert voiced concern that the presented targeting approach might still not comply with the requirements set out by the CJEU on data retention.

On proportionality safeguards, the Member States in question explained how these also required rules on targeted access, i.e. differentiated access depending on the requesting authority (intelligence services, judiciary, ...). Some MSs suggested that targeting could be done at access level, rather than at the moment of retention.

Service providers highlighted the need for a stable legal system, ideally harmonised across the EU, so that the implementation work would not end up being a sunk cost, especially in view of the remaining risk of an investment. They called for a solution that can pass the scrutiny of the Court.

Experts stressed the importance of allocating responsibilities to all the operators (including OTTs) to ensure that competent authorities can request (upon appropriate judicial authorisation) specific categories of data (i.e., needed to identify or locate a subject) and SPs must comply, irrespective to the type of service they offer.

Experts also discussed the need for defining what data service providers hold, and noted that providers frequently change these data types, hence technological neutrality is difficult to attain across data sets. It was suggested by some Members of the WG that it would be more efficient (as it is the case in some national legislations) to use specific use case for the data (identification of the origin of the communication, identification of the location of the mobile equipment, etc).

Experts called for data collection in those countries where targeted retention would only cover part of the country to determine how many investigations come up empty and whether criminals make proactive use of the "blind spots" created by the geographic zones (which are public).

Experts noted that the long-awaited e-evidence package is expected to be a game changer for access to data retained by the major ISPs and called for a timely and sound implementation of those rules.

2. Capacity building

In this session, experts discussed the feasibility of applying standardised formats for accessing data and potential solutions for enhancing Member States' capacities to access digital evidence.

A representative from standardisation institute (ETSI), invited the experts to contribute to the work of ETSI's relevant WGs, in order to define together, also with CSPs and OTTs, the data types which could then be used by the law enforcement community. Using the same standards would facilitate achieving technology neutral solutions and including emerging sectors (such as automotive).

New standards would also be necessary to ensure that Internet Service Providers can implement the relevant mechanisms for targeted retention and access based on agreed criteria .

Most of the participants agreed that an EU wide solution would harmonize and level the playing field across MSs and would also be beneficial for the effective and proper functioning of the e-evidence package.

3. Cooperation with Service Providers

Experts discussed possible mechanisms for fostering cooperation with communication and technology providers. A representative from ETNO presented the areas where enhanced cooperation would be needed. These included the need for automation of processes (ETSI) to allow operators to comply with the rules, compensation for the implementation of harmonised rules.

Experts discussed the need to clarify the rules and terms for retention, including the need to have clear established criteria for data collection which should not be left to the operators' discretion.

Experts recognised the major role of the SIRIUS project hosted by Europol to support this cooperation and suggested to further build on this mechanism.

	AVENUES TO EXPLORE	POTENTIAL SOLUTIONS
HARMONISATION / LEGISLATIVE APPROACHES	Developing Union policies and exploring legislation on data retention to: ▪ reduce the impact of fragmentation of data retention frameworks for lawful access to data by law enforcement authorities by exploring the possibilities compatible with the Charter and the CJEU case-law; ▪ clarify the interplay of data retention with data protection rules (GDPR/LED), ePrivacy and the e-evidence package; ▪ address open challenges such as non-unique IP addresses lack of geolocation or encryption; ▪ create a level playing field for all electronic communication service providers, including OTTs.	▪ Harmonisation across the EU of rules and safeguards regarding data availability, retention, and access to raw data. ▪ Enforcement of a level playing field for all communication service providers, including OTTs, on retention requirements.
CAPACITY BUILDING	▪ Establishing standardised formats for data retention and access, based on ETSI standards (notably for categories of data currently not covered by standards). ▪ Establishing standardised and secured channels for exchanges with SPs via the e-evidence exchange system. ▪ Fostering the development of MS capacities to access, exchange, and process digital evidence	▪ 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).

COOPERATION WITH INDUSTRY \ STANDARDISATION	▪ Reflect on mechanisms for a robust cooperation with communication and technology providers e.g., to increase transparency and better address technological shifts.	▪ 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).