Working Group 3, Access to data in transit

Request for input from experts

To date, two meetings of the Working Group 3 of the High-level Group (HLG) on access to data for effective law enforcement, focused on access to **data in transit**, have taken place on 4 October 2023 and on 13 February 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 10 April will allow the experts to prepare draft recommendations to address the identified challenges and drivers/legal constraints. The experts' recommendations will then be presented at the Plenary meeting on 21 May.

To this end, experts are kindly requested to provide at least one recommendation for each of the solution areas that are being explored, namely lawful interception, lawful remote access of intrusive nature, and challenges linked to encryption. The overall contribution should consist of a maximum of 2 pages of potential recommendations and, where relevant, should flag whether suggested solutions refer to the domain of capacity building, international cooperation/standardisation or legislation. Contributions should be sent to EC-HLG-GOING-DARK@ec.europa.eu by Monday 8 April the latest.

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 potential avenues for solutions identified in previous meetings**. In addition, experts will find the presentations delivered during the meetings of the working group in the Workspace for the experts of the HLG as well as relevant documents transmitted by experts outside of the meetings.

SUMMARY OF PREVIOUS MEETINGS

Working Group 3 (WG3) met for the first time in October 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 in transit.

On challenges:

- While **lawful interception remains an essential tool in many investigations**, **the efficiency of this measure has drastically decreased in the past 15 years**, with now – according to experts - around 80 to 90% of the traffic being encrypted, thus rendering the exploitation of data extremely challenging from an investigative perspective. In addition, experts confirmed that most interpersonal communications are now carried by non-traditional communication operators, that do not provide for real time lawful access capabilities[1].

[1] A practitioner mentioned an example where the target was under surveillance during more than 6 months but never made a traditional phone call or SMS.

- This significant loss in access to data in transit affects investigations in several ways:
    - an increased difficulty in many cases to map organised crime groups and activities and identify high value targets[2],
    - an increased use of so-called special techniques that are often more intrusive (e.g. where the judicial authority prescribes the installation of cameras or microphones close to the target) and more dangerous for the officers in charge;
    - an increased usage of investigation techniques that are less targeted, e.g. without access to content of communication investigators often have to investigate a greater number of persons in relation with an individual suspected of criminal activities.

- Encryption also **affects real time access to meta-data** that, in addition, are often less present in providers' systems (see Working Group 2).

- Criminals have adjusted their communication habits in response to law enforcement's ability to intercept. They first moved from traditional communication service providers (CSP) to regular Over the Top (OTT) communication providers, then to specialized criminal communication networks (such as Encrochat and Sky ECC) and **recently moved back to regular OTTs**, where they feel they are currently not at risk.

- **Member States have thus far not been able to enforce obligations on OTTs on real time access to communication**, despite some of them[3] setting regulations that provide for such legal requests. Several experts from law enforcement and the judiciary expressed concerns on the current discrepancy between CSPs and OTTs concerning the implementation of legal obligations pertaining to lawful access[4].

- Challenges on real time lawful access are **not limited to OTTs**. Other challenges include:
    - RCS (Rich Communication Services) that is becoming the norm to exchange SMS in an end-to-end encrypted manner,
    - 5G communications for inbound roamers (when the targets are using SIM cards issued by foreign operators),

- Operations such as Encrochat or Sky ECC are strongly challenged in courts. Legal uncertainty results notably from the very different requirements across national legislations when it comes to taking the outcome of an intercept in one member state and making use of them in another.

- International cooperation on real time access to communication brings technical and legal challenges. In practice, such measures implemented through MLA or EIO are often incompatible with the pace of an investigation.

On the way forward:

- While being convinced that dedicated criminal communication networks will still exist in the future, experts pointed out that **the focus of this group should be on accessing real time communication at OTT level** and, from a more forward-looking perspective, on maintaining lawful interception capabilities for traditional telecommunication operators despite 5G and 6G expected in 2030.
- Experts insisted that **lawful interception of electronic communications services should be the privileged measure to access data in real time**, provided that they are authorized by law, in line with technical standards and with relevant safeguards on data protection and privacy,

[2] As illustrated by ES representatives with operations TENEDOR and ESCAMA, where only the information provided by SKY ECC and Encrochat allowed progress in the investigation, leading to the arrest of several high value targets.

[3] E.g. BE, FR.

[4] For some MS, legal obligations on lawful access are similar for CSPs and OTTs, however a local lawful interception request will be set up in a matter of hours for a CSP and in matter of months (if ever) for an OTTs (through an MLA).

cybersecurity and interoperability measures. Such lawful interception should be based on principles that currently apply for lawful interception of traditional communication providers for example in terms of oversight and cooperation with operators of communications.

- While **access by means of special techniques remains relevant, it should be the exception** considering the high technical, legal and ethical challenges associated to the use of intrusive technologies. In addition, the exploitation of vulnerabilities to get access to evidence often implies secrecy on how those techniques work, which conflicts with the principle of explainability that prevails in forensic activities. Moreover, the usage of vulnerabilities is potentially in contradiction with cybersecurity principles (e.g. on vulnerability disclosure), unless subject to well-defined vulnerabilities equities processes.
- On **accessing content data despite encryption**, experts expressed the wish **to explore first technical aspects,** in coordination with cybersecurity experts. In addition, security experts expressed the need for standardisation to address law enforcement's operational requirements, notably in new telecommunication standards such as 6G.

In the previous meeting of WG3, on 19 February 2024, experts structured the discussions on possible solutions along three strands:

1. Lawful interception
2. Intrusive measures
3. The challenge of encryption

The table below summarizes the possible avenues to explore identified during this meeting (A summary of discussions is annexed).

	AVENUES TO EXPLORE SUGGESTED BY EXPERTS
Lawful interception of electronic communications services	▪ Legal: • share a common understanding of what is legally sound under the EECC, and ePD • foster harmonization/approximation of national laws based on guiding principles (e.g. in relation with admissibility checks by service providers, with the geolocation of users and/or infrastructures) • explore a scheme based on the European Investigation Order: • what would be needed to enable lawful interception for OTTs (e.g. based in Ireland)? • would such scheme respond to the needs expressed by security practitioners e.g. in terms of reactivity? • explore the creation of new obligations for electronic services providers building on some of the principles set out in the e-evidence package, • explore the creation of specific obligations for electronic service providers e.g. when datacentres are located in the demanding country, it should be possible to set up an interception measure without going through a cross border cooperation instrument, ▪ Technical: • explore the definition of a relevant technical capability for near real time lawful interception of the main Internet Service Providers, • further develop standards targeted to OTTs, • improve mechanisms for an accurate geolocation of users,

	▪ Cooperation/standardisation: • foster the uptake of standards by electronic communications providers, • increase transparency on the implementation of lawful interception mechanisms including oversight,
Lawful access to data handled by non-cooperative service providers	▪ Reflect on criteria to determine what is a non-cooperative or criminal communication provider, ▪ Work on possible sanctions / blocking measures that could apply for non-compliant providers, ▪ Work on a coordinated approach on harmful hosting providers (see document on the approach envisaged at national level by the Netherlands on the platform), ▪ Work on admissibility of evidence for receiving states (when data is acquired by means of intrusive measures), ▪ Reflect on safeguards pertaining to the development, acquisition and usage of intrusive tools, and work on guidance to use those tools (off meeting, experts referred to the international initiative called "Pall Mall Process" aiming at tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities), ▪ Work on a process for a sound management of vulnerabilities (such as vulnerability equity process in the US) in collaboration with cybersecurity authorities and limited to judicial investigation.
Challenges of encryption	▪ Increase efforts on standardisation and capacity building in relation with decryption (tools, trainings and research notably in the area of quantum computing) ▪ Identify short-term mitigation measures for current challenges, such as possible solutions to mitigate the *home-routing* challenge (i.e. the inability to intercept users with foreign sim cards see presentation by Europol), Rich Communication Services (RCS) or satellite-based communications, ▪ Agree on a definition of operational needs that could serve as a reference for future technological, standardisation and policy developments, based on the Law Enforcement Operational Needs (LEON) document. ▪ Outline an approach to address through standards the challenge of lawful access by design without weakening or undermining encryption or indiscriminately affecting the privacy of all users of a service.

ANNEX – HLG WG3 – 19 February 2024 - Summary of discussions

1. Lawful interception of Over The Top communication providers (OTTs)

Participants from OTTs and national authorities agreed that Member States are currently not in the position to enforce lawful interception obligations on OTTs. They overall agreed that this is notably due to conflicts of law creating legal uncertainty. In response, experts discussed various policy avenues for a possible lawful interception scheme that would apply to all forms of electronic communications providers and be compatible with law enforcement and judicial needs. Such possible avenues could include:

- Legal:
    - harmonization of national laws based on common principles,
    - adjustment of cooperation instruments (e.g. EIO),
    - creation of new obligations for electronic service providers building on principles set out in the e-evidence rules/package,
    - creation of new obligations for electronic service providers based on the location of datacentres,
- Technical:
    - further developing standards targeted to OTTs,
    - improving mechanisms for an accurate geolocation of users,
- Cooperation:
    - foster uptake of standards,
    - increase transparency,
    - work jointly on technical and operational solutions.

In more detail:

- Experts agreed on the necessity to work primarily with OTTs on a **legitimate** access channel (i.e. through a lawful interception management system (LIMF)), based on principles that exist already for lawful interception of traditional communication providers.
- Police/Justice experts would like the operators to be able from the time they receive a legal request from the authorities, to deliver data **for the future**. There is no request to get access to data that was exchanged before the legal order.
- Microsoft explained that the problem is **more legal than technical** (except on encryption). As an illustration, Microsoft referred to the technical work already conducted to develop lawful interception in real time capabilities of for Skype calls or Teams services.
- Interoperability is fundamental at EU level to address disparity amongst MS LI systems; it can be achieved through standards already under development (such as ETSI 103.120)
- Experts from both sides consider that the work should primarily address legal issues such as the EIO not applicable in Ireland, potential unnecessary legality checks by OTTs, conflict of laws, unclarity on extraterritoriality issues, explore the possibility to directly address entities with data centres located in the EU, etc...
- The question of location is considered essential. The legal implication of the location of users should be clarified. The technical ability to get access to precise real time geolocation should be a priority as it will contribute to provide legal certainty.
- Experts recalled that MLA/EIO do not meet law enforcement operational needs: too slow and not direct.
- Experts mentioned the need to build at the same time a framework for non-compliant electronic communications services as otherwise it would create an uneven playing field among actors that would impact business and security [see point 2 below]

2. Access to data handled by non-cooperative communication providers.

In cases like Encrochat and SkyECC, communication providers were identified by judicial authorities as supporting solely or mainly criminal activities. In the future, alike communication providers will still exist, and are unlikely to comply with any obligations on LI. In addition, other communication networks, due to their decentralized management or lack of clear ownership are also unlikely to comply voluntarily with Member States' or - potentially - with EU obligations on lawful interception.

Experts put forward avenues for possible initiatives, including:

- Agree on objective criteria to determine what is a non-cooperative or criminal communication provider,
- Work on possible sanctions / blocking measures that could apply for non-compliant providers,
- Work on a coordinated approach on harmful hosting providers (see document presenting the approach envisaged at national level by the Netherlands on the platform),
- Work on admissibility of evidence for receiving states (when data is acquired by means of intrusive measures),
- Reflect on safeguards pertaining to the development, acquisition and usage of intrusive tools, and work on guidance to use those tools,
- Work on a vulnerability equity process in collaboration with cybersecurity authorities.

In more detail:

- Magistrates involved in EncroChat and SkyEcc detailed the technical and legal background that made those operations possible.
- Notably FR laws provide for its jurisdiction over hosting providers located in France or data transmitted via a France-based service provider and thus legal certainty on access to data irrelevant of the location of the data owner.
- If such conditions are not met (e.g. criminal hosting provider located in another MS) what should be done:
  - Block the application from being downloaded?
  - Criminalize non-cooperation of data centres?
  - Use hacking tools?
- An expert suggested avenues to reinforce the admissibility of evidence from the receiving state's perspective:
  - define the conditions for authorising the interception of large-scale communications;
  - strengthen the content of the judge's authorisation decree;
  - reflect on mandatory destruction of "irrelevant" material;
  - strengthen procedures to ensure sound acquisition of digital data to certify authenticity and integrity.
- Experts discussed the need to reflect on guarantees and safeguards when MS are using special technics that exploit vulnerabilities, including oversight, evaluation and certification of the tools as well as the virtue of a vulnerability management scheme.

3. Challenges of encryption

Encryption adds a level of complexity when it comes to accessing real time content data, both for OTTs when implementing an end-to-end encryption mechanism and for traditional telecommunication operators for example when implementing of "Home Routing" in 5G.

Experts gave an outlook on the capacity to take concrete steps by:

- Identifying short-term mitigation measures on the technical side, such as possible solutions to mitigate the *home-routing* issue (i.e. the inability to intercept users with foreign SIM cards),
- Agreeing on an EU definition of operational needs that will serve as a reference for future technological, standardisation and policy developments, based on the Law Enforcement Operational Needs (LEON) document.
- Outlining an approach to address through standards the development of communication technologies that would enable lawful access without weakening cybersecurity mechanisms. This approach, that shall involve the evaluation and certification of lawful interception systems, opens a perspective in the longer term and for upcoming technologies such as 6G.

In more detail:

- On the specific challenge of "**Home Routing**" (i.e. when a 4G/5G user with a SIM from a foreign communication provider cannot be intercepted), Europol suggested short term measures building on cooperation agreements and organisational measures, as well as long term measures. The latter would be based on clear rules to guarantee- through specific agreements- lawful interception of data in clear by disabling when needed certain mechanisms (paper to be produced).
- On standardisation.
    - Experts discussed an approach based on technological solutions that should be standardised, evaluated, and certified by national/European authorities.
    - Experts outlined a path to develop EU standards that are needed to develop secured technologies that factors in lawful access requirements.
    - Such approach should involve cybersecurity experts and include strong identity management (eIDAS high level) as well as certified cryptography mechanisms (e.g. identity-based encryption, homomorphic encryption including quantum safe computing)
    - It should be directly driven by the commission through standardisation requests.
    - Experts called for an EU recommendation to implement the needs described in LEON in national legislation.
    - Technical standardization: experts should be able to refer to LEON as guidelines in technical discussions in standardisation committees.