High Level Group
on Access to Data for Effective Law Enforcement

Working Group 3 - 1st meeting - 4 October 2023

Real time access to data in transit

Background document

Introduction

Criminals, like anyone else, depend more and more on communication systems to develop their activities. They frequently take advantage of opportunities offered by broadband communications systems to make arrangements among themselves and to commit offences while seeking to avoid detection. In that context, real time access to data in motion remains an essential tool for the fight against serious crime developing online and organised crime as well as counter-terrorism.

Lawful interception, as the primary instrument for real time access to data in motion, is a national matter in essence. Most Member States have in place dedicated national regulatory frameworks for real time collection of communication data, which vary significantly amongst them[1]. From a legal perspective, Member States can set obligations on communication service operators for real time access to data in transit, within the boundaries set by EU Law, notably the EU Charter of fundamental right and the ePrivacy Directive[2], which allows for proportionate exemptions from the rule of confidentiality of communications notably for the purposes of prevention, investigation, detection and prosecution of criminal offences, and the new European Electronic Communications Code (EECC[3]), which allows Member States to impose obligations on operators of communication networks and services in compliance with the ePrivacy Directive and the GDPR. This legal framework is complemented by the Budapest Convention and its additional protocols and by the Directive on Attacks Against Information Systems,[4] both of which criminalize unlawful interception of communication. Furthermore, the Directive regarding the European Investigation

[1] For example, in terms of threshold to authorize such measures.
[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[3] Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code
[4] DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems

Order in criminal matters allows to issue an EIO for the interception of telecommunications via the technical assistance of another Member State[5].

The way in which telecommunications were organised until recently, structured around large national operators, fitted well with an approach on lawful interception taken strictly at national level. The progressive shift to the world of Internet communication services is a game-changer, with new players coming into the picture. It poses new challenges as often communications are not treated locally and communication protocols are becoming more diverse and harder to handle by national authorities, notably with the development of end-to-end encrypted services.

In addition, operations conducted on networks specifically designed to provide anonymity for illicit purposes, such as Encrochat, Sky ECC or ANOM networks, demonstrated the need for international cooperation and a solid legal framework to tackle such phenomenon, as traditional methods to obtain access to real time data communication data and metadata cannot apply.

Against this background, a reflection is needed to identify the challenges faced by Member States' authorities to maintain the necessary capability for real time access to data in transit and explore EU-wide avenues in a forward-looking perspective. This reflection should be carefully balanced to ensure that access related measures to prevent and deter criminal activities are designed and applied in full respect of the EU Charter for Fundamental Rights, and the applicable secondary legislation such as the data protection and privacy framework and include appropriate judicial procedural safeguards.

Taking stock

In view of the above, as the first step, Working Group 3 will take stock of the current situation, namely by inviting law enforcement practitioners to present their operational need for lawful access to data in transit as well as possible obstacles, challenges and/or current legal constraints. Experts are also invited to present their perspectives on the possibilities to ensure that such measures are undertaken in compliance with fundamental rights and cybersecurity requirements.

Accordingly, the members of the Working Group 3 are invited to contribute in writing a typical case scenario for access to data in transit in real time. They are also invited to indicate possible challenges and capacity gaps that law enforcement authorities face, or will face in the foreseeable future, regarding real time access to data in transit, in particular those that have an impact on law enforcement work.

[5] On the potential scope of request for interception see e.g. recital 30 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36: Possibilities to cooperate under the EIO Directive are '*not limited to the content of the telecommunications, but could also cover collection of traffic and location data associated with such telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications*'.

Members may structure their contributions on the basis of the questions below. They are encouraged for the sake of clarity to distinguish, when relevant, between the use cases and challenges pertaining to widely used communication services (e.g. based on new protocols such as Rich Communication Services (RCS), or communication applications such as WhatsApp, Signal, or iMessage) on one hand and ad-hoc communication services operated to serve primarily criminal purposes, such as the former Encrochat network, on the other hand.

In their analysis, participants should consider the national implementation of the European Electronic Communication Code, the e-evidence package, as well as existing possibilities for requesting the interception of telecommunications by another Member State through an EIO.

The cases should be submitted by 29 September 2023 to the following e-mail: EC-HLG-GOING-DARK@ec.europa.eu with the subject: *Cases Working Group 3*.

While submitting, please indicate whether you would be interested in presenting the submitted case and/or identified challenges at the Working Group 3 meeting on 4 October 2023.

Discussion questions

The presentations will be followed by a discussion based on the following questions:

Morning session

1. *In which types of cases must law enforcement authorities access data in transit in real time in communication systems, for those cases to be effectively prevented, detected, investigated and prosecuted?*
2. *What is the practitioners' experience with their national lawful interception regime as regards non-traditional telecommunication operators[6], notably in light of the national implementation of the new European Electronic Telecommunication Code? How does this interception regime for non-traditional telecommunication operators differ from that for traditional operators? Are law enforcement needs similar with regards to both?*
3. *Could you describe and illustrate cases where real time access to data in transit was necessary but turned out to be difficult or impossible for legal or technical reasons (please specify which were the legal/technical reasons) as well as the impact on the investigation and prosecution of serious crime? Could you explain how such cases have, in lieu, been solved through other means, if so[7]?*
4. *In the context of lawful interception, which categories of data (metadata/content data, other categories) are necessary to effectively investigate and prosecute criminal offences?*

[6] As opposed to «telecommunications carriers". These companies provide various communication services, including voice calls, text messaging, data services, television and internet services.

[7] If the judicial proceedings are still ongoing the cases should be considered as "pending before the courts"

Afternoon session

1. *What are the technical challenges and capacity gaps or legal constraints – if any – that national authorities face or will face in the foreseeable future regarding lawful interception of data in transit where communications are provided by legitimate operators for public use?*
2. *What are the challenges, capacity gaps or constraints – if any – that national authorities will face in the foreseeable future to fight criminal activities developing on encrypted communication networks specifically designed to support criminal activities, such as Encrochat or Sky ECC?*
3. *Do any of those challenges identified affect cross-border or international police and judicial cooperation? If so, in what way concretely?*