sweden 2023.eu Swedish Presidency of the Council of the European Union

European Commission

Background document

Operational challenges faced by law enforcement related to access to data

Input to the first plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement

Law enforcement authorities need to effectively and lawfully carry out their tasks to investigate and prosecute crime, provide justice to victims of crime and safeguard public security. Data digitally generated or stored is an increasingly important component of nowadays criminal investigations. The access to this information for law enforcement purposes can affect the fundamental rights of individuals. Therefore, any access and use of such data must be necessary and proportionate to the purposes of law enforcement. It shall be accompanied by appropriate procedural safeguards, be subject to judicial review, and respect the relevant Union law and its interpretation by the European Court of Justice.

In this context, law enforcement authorities face operational challenges which this paper tries to illustrate and map in a simple and concise manner as a basis for discussion, to stimulate the interactive participation of all stakeholders and the sharing of different perspectives.

When referring to access to data by law enforcement, this paper refers to lawful access to data.

1. Types of data

The HLG will explore the problems that law enforcement practitioners face when trying to access data that they require to perform their tasks. This concerns in particular:

- **Communications metadata** (IP addresses, traffic, and location information). This concerns all data needed to identify users, and to determine who has communicated with whom, when, where and through which means of communication.
- **Communications content data** (data exchanged between the communication partners in a digital format, such as text, voice, videos, images, and sound).

Access means that the digital information exchanged is available to law enforcement in a **readable** format.

2. Use cases

Obtaining adequate access to these types of data presents different challenges to law enforcement, depending on the following distinct **use cases:**

1. Access to **data at rest in a user's device**
2. Access to **data at rest in a provider's system**
3. Access to **data in transit** ('real time access')

For each use case law enforcement practitioners require access to either communications metadata or communications content data or both.

Access to this data, whether already stored and available or still to be collected through specific investigative measures, is understood as access granted to law enforcement subject to judicial authorisation in the context of criminal investigations and on a case-by-case basis. As a rule, such judicial authorisation is necessary due to the sensitive nature of the data in question and represents an integral part of the applicable legal and operational framework for facilitating access to this data by law enforcement.

3. Challenges

When trying to access communication data or content data in any of these three use cases, law enforcement practitioners are confronted with one or more of the following challenges:

- The data is not stored / is not retained
- The data is encrypted
- The data is not released by the service provider[1]

Depending on the use case, the following law enforcement challenges shall be explored and discussed:

	Challenges		
Use cases	Data is not stored / is not retained	Data is encrypted	Data is not released by the service provider
<u>Use case 1:</u> Access to data at rest in a user's device		**X**	
<u>Use case 2</u>: Access to data at rest in a provider's system	**X**	**X**	**X**
<u>Use case 3</u>: Access to data in transit ('real time access')		**X**	**X**

The articulation of a specific challenge will be different, depending on the use case. As an example, the encryption challenges that law enforcement practitioners must tackle when accessing data at rest on a device are different from encryption challenges in relation to data in transit.

[1] Depending on the technology used, the data may even be unavailable to the service provider.

4.1. Challenges concerning data at rest in a user's device

Data at rest in a user's device refers to both communication metadata and content data physically housed in any digital form on an electronic data storage (e.g., mobile device, computer or USB stick) in the possession of an end-user.

4.1.1. Data is password protected or encrypted

Modern devices are encrypted by default[2], to ensure security and confidentiality. This technical safeguard can also make users' data unreadable for law enforcement. In such case, law enforcement only has two options: getting access to the user's password (or equivalent) or breaking encryption. In recent years, hardware manufacturers have added hardware security modules to prevent access to decryption keys, making access to encrypted data even more challenging.

In that context, accessing encrypted data in a readable format is time-consuming, costly, requires advanced technical capabilities and is often even impossible for law enforcement.

> Example
>
> An Apple laptop was seized by police in a suspect's residence, in the context of a criminal investigation. IT forensic experts search for evidence in this device. However, they cannot obtain the evidence because Apple laptop devices are encrypted by default with built-in security features that prevent access by third parties, including access by law enforcement in possession of the latest digital forensic tools available on the market as well as advanced techniques.
>
> The same issue may arise with other devices (personal computers, hard drives, USB keys, mobile phones).

4.2. Challenges concerning data at rest in a provider's system

Data at rest in a providers' system refers to communications metadata or content data housed by a service provider in its systems (either in the traditional communication provider's system like Orange, or in cloud storage such as Google cloud).

4.2.1. Data is not stored or is not retained

Access to communications metadata or content data at rest in a provider's system can nowadays be pivotal for almost all criminal investigations, especially in establishing the identity of suspects or persons of interest who may have relevant information, which is a critical objective in criminal investigations. Especially for crimes committed via the internet, communications metadata (notably the IP address) may sometimes be the only way to identify a suspect.

Such information is accessible to law enforcement only if it is available (i.e., retained) by the provider.

[2] Encryption by default is often a feature of the operating system. Devices running on various versions of MacOS, Windows, IOS or Android include this feature.

However, depending on the commercial need to retain data and/or national requirements, while some internet service providers (ISP) store communications metadata, others do not. In addition, when communication metadata is stored, the retention period varies and such period might be short. Moreover, specialised companies offering anonymisation services such as VPN[3] often do not store subscriber's data[4] nor communication metadata. Finally, hosting services allow users to rent servers using fictitious data[5].

As a consequence, the absence of stored data and the anonymisation services make it difficult or even impossible in some cases to identify a suspect or a person who may have relevant information ('subject of interest') in a criminal investigation. In addition, in some cases, the ability of law enforcement to execute targeted investigative measures, such as lawful interception of communications is reduced, because in order to obtain a judicial decision for these measures, there must be an identifier like an IP address.

Example

A Member States' law enforcement agency receives a report from a private party containing information regarding a potential serious crime offence. The report includes information that an IP address from that Member State was used to perpetrate the crime.

If the ISP who holds the IP address is in possession of information about who used this IP address at a certain time (subscriber information), law enforcement can request subscriber information from the ISP.

The ISP may answer in three different ways:

1. One name provided. The ISP has stored data on the specific subscriber who was using the IP address at the time and provides the name to the law enforcement agency. The information points towards a suspect and the investigation can move forward.
2. Many names provided. The ISP stored data on who was using the IP address at the specific time. However, the IP address was provided by the ISP by means of Network Access Translation (NAT)[6]. The ISP may provide the law enforcement agency with a list of all the names of individuals using the IP address at the time. The law enforcement agency must take further measures to identify the suspect.
3. No name provided. The ISP is unable to provide a name on who was using the IP address at the specific time.

[3] VPN ('Virtual Private Network') enables the user to establish a protected network connection when using public networks. VPN encrypt internet traffic and disguise the user' online identity.

[4] Subscriber data is all information and data relating to subscriber including subscriber's name, addresses, and email addresses.

[5] https://en.wikipedia.org/wiki/Bulletproof_hosting

[6] When using NAT, several users use the same IP address to connect to the internet. Theoretically, 64 000 users could share the same IP address by means of NAT.

The reason for the service provider not providing the name may be:

a. The ISP does not store data on which user is using a particular IP address and cannot provide a name to law enforcement.

b. The ISP only stores data on which users are using a specific IP address during a limited time. When the retention period has expired, the data is deleted.

c. The data may be anonymised using a VPN service that do not retain subscriber and communications metadata.

4.2.2. Data is encrypted

Content data at rest in providers' systems may also advance criminal investigations. Nowadays, communication applications like WhatsApp or cloud storage services provide end-to-end encryption (E2EE). Some encryption techniques allow the service provider to access content data, however, techniques such as E2EE often make access impossible even for the service provider.

<u>Example</u>

A law enforcement agency requests cloud backups of instant messages in the context of a criminal investigation. However, the cloud storage is end-to-end-encrypted in that specific service, and the ISP cannot provide the law enforcement agency with the requested content data in an unencrypted i.e., readable format.

4.2.3. Data is not released by the service provider

Service providers may hold communications metadata or content data that they do not (wish to) release to law enforcement, referring to their terms of service that do not allow for that. This may depend to the kind of service provided or the specific policies of the provider.

4.3. Challenges concerning data in transit

There are also challenges in connection with real time access to communications metadata and content data, which are in transit, namely data in motion between source and destination.

4.3.1. Data is encrypted

Content data communicated in the context of communication services offered by OTT (Over-The-Top) communication providers[7] can be encrypted with E2EE. Law enforcement cannot enforce real time measures to access this encrypted content data.

<u>Example</u>

In the context of a criminal investigation conducted by the police, the judicial authorities authorised the real time investigative measure of lawful interception

[7] OTT can include instance messaging services or online chat. It also includes voice calling capabilities called VoIP (Voice-over-IP).

of communications of a suspect of a serious criminal offence. The suspect is communicating mostly through Signal and WhatsApp end-to-end encrypted messaging systems.

In case the communication service is end-to-end-encrypted, the service provider is unable to provide the law enforcement agency with the content data. In the best-case scenario, the service provider may be able to provide law enforcement with communications metadata that answer only to whom, where when and how the suspect is communicating, but not the content of the communication. As an additional challenge, technical mechanisms to enable the provision of such information in real time are often not in place in the OTT (see 4.3.2).

Example

In the context of fighting organised crime, law enforcement agencies have identified several criminal groups using similar encrypted communication devices, specifically designed to provide extra layers of encryption and anonymity[8] for criminal use such as Encrochat. The law enforcement eventually got access to communications metadata and content data of identified criminals by breaking into the encrypted communication networks. Such operations however require cutting edge technical capacities which may not always be available and pose a number of specific legal challenges[9].

4.3.2. Data is not released by the service provider

While much of the interpersonal communication is handled today by OTTs, in most cases only traditional telecommunication providers[10] have the technical infrastructure in place that provides for real time lawful interception of communication. Hence, although it might be legally possible for judicial authorities to request the data, some providers are (technically) not able to provide the data. In that context, irrespective of end-to-end encryption features, it may not be possible for law enforcement services to execute an interception for communication channels handled by OTT providers sine the necessary technical infrastructure is not in place.

Example

In the context of a criminal investigation conducted by the police, the judicial authorities authorised the real time lawful interception of communications of a person suspected of having committed a serious criminal offence using WhatsApp services. The request for lawful interception was sent to the traditional telecommunication provider (e.g., Orange) of the suspect. The traditional telecommunication provider would technically have been only able to provide access to communications metadata.

[8] https://www.eurojust.europa.eu/fr/document/joint-eurojust-europol-press-release-encrochat-case

[9] https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)739268

[10] The operators’ telecommunication infrastructures that have been allocated frequency for 3G/4G/5G communication.