High Level Group
on access to data for effective law enforcement

Working Group 1

Access to data
at rest in a user's device

Background document

19 July 2023

1. Introduction

Law enforcement authorities need to carry out their tasks effectively and lawfully and in respect of fundamental rights to prevent, detect, investigate, and ensure the prosecution of crimes, to provide justice to victims, and safeguard public security.

Digitally generated or stored communication data (both metadata and content data) is an increasingly important component of modern criminal investigations. Access to this data by law enforcement is understood as access granted to law enforcement subject to judicial authorisation and supervision in the context of criminal investigations and granted on a case-by-case basis. Such judicial authorisation is necessary due to the sensitive nature of the communication data in question.

Law enforcement authorities face increasing operational challenges when seeking to lawfully accessing data digitally generated 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.

In its first plenary meeting of 19 June 2023, the High-Level Group on Access to Data (HLG) has established three separate working groups to explore the above use cases in further detail.

The first working group ('Working Group 1') is tasked to focus on access to data at rest in a user's device[1]. It will meet (at least) three times in the framework of the High-Level Group.

The Working Group 1 first meeting (19 July 2023) will take stock of the current situation and focus on identifying and prioritising the main challenges encountered by law enforcement, and the drivers that underpin them, while the Working Group 1 second meeting (date TBC 2023) will focus on identifying possible solutions, and the Working Group 1 third meeting (date TBC 2024) on formulating possible recommendations.

After each meeting, the Working Groups will report their findings to the next plenary meeting of the High-Level Group.

The present background document provides a basis for discussion and has the objective of stimulating the interactive participation of all stakeholders and the sharing of different perspectives during the Working Group meetings.

---

[1] Data at rest in a user's device refers to both communication metadata and content data physically stored in any digital form on an electronic data storage (e.g., mobile device, computer or USB stick) in the possession of an end-user. Accessing data at rest includes all cases where the device is in physical possession of law enforcement authorities. It does not concern the possible remote access to the device by law enforcement, which will be covered in the Expert Working Group 3 on data in transit.

2. Typical use cases for lawful access to data at rest in a use's device

The objective of this section is to describe typical use cases where law enforcement authorities seek to access data at rest in a user's device in the context of a criminal investigation, to identify different typologies of situations and challenges faced. All the below examples pre-suppose that national law enforcement authorities act under the supervision of judicial authorities, and with the necessary judicial authorisation to act, as the case may be.

Use case 1: Law enforcement authorities arrive on a crime scene, where a victim is found dead with five gunshots, with a smartphone and laptop next to him inside the room. The devices are seized. They are password protected and the passwords are not known or available.

The analysis of the devices can be instrumental to identify the relations and the activities of the victim, which can lead to the identification of the person(s) suspected of perpetrating the homicide. Depending on the specificities and requirements of this investigation (e.g., other evidence available, potential suspects etc.), data such as the victim's communications (e.g., emails, instant messages, photos, or videos sent or received via the seized devices of the victim, as well as GPS data) may need to be searched, extracted, and analysed.

For this purpose, the seized laptop and smartphone are sent to the forensics laboratory for digital forensic investigation.

Use case 2: A law enforcement authority that investigates a drug trafficking case searches the residence of a person suspected of dealing drugs, following a judicial authorisation, in accordance with national law. The suspect is present, and 10 smartphones are found inside the house, including iPhones, and Google Pixel phones, as well as an unknown type of smartphone. Most phones are powered off. The suspect refuses to provide the password to all these devices and any information about the unknown smartphone.

The analysis of the devices can be pivotal to establish the relations and the activities of the suspect, which can lead to the establishment of the suspected criminal offence (drug trafficking), and specific circumstances such as how long the suspect was selling drugs for, the suppliers, accomplices, drug hiding places, etc. Depending on the specificities and requirements of this particular investigation (e.g., other evidence available like surveillance footage etc.), data like the suspected drug dealer's communications (e.g., emails, instant messages, photos, or videos sent or received via the seized devices, as well as GPS data) may need to be searched, extracted, and analysed.

Nine of the seized smartphones are known and commercially available phones with encryption capabilities (e.g., iPhones) and one of them is an unknown smartphone that can be bought using cryptocurrencies and is marketed in the dark web as an undetectable and untraceable communication device offering anonymity and confidentiality for criminal purposes.

For this purpose, the seized smartphones are sent to the forensics laboratory for digital forensic investigation.

Use case 3: A law enforcement authority that investigates a child sexual exploitation network, searches the residence of a suspected child sexual offender, following a judicial authorisation, in accordance with national law. The law enforcement authority discovers and seizes several laptops and tablets, and USB sticks in the premises of the suspect. The suspect is present during the house search but refuses to provide the password for those devices. The laptops are equipped with TPM (Trusted Platform Module) chips[2], some hard drives are encrypted with Bitlocker[3], others are encrypted with LUKS (Linux Unified Key Setup)[4].

Some files on the USB sticks are password protected / encrypted, including with PGP (Pretty Good Privacy)[5] and VeraCrypt[6] software. Altogether, investigators seize more than 100 TB of data.

Depending on the specificities and requirements of this investigation (e.g., other evidence available such as lawful interception, etc.), emails, photos, or videos sent or received via the seized devices of the suspect, traces of access to child abuse material distribution networks, including live streaming networks, P2P[7] networks and Darknet networks) may need to be searched, extracted, and analysed. The investigators may ask specific questions to the forensics laboratory that point to specific data required for the investigation (e.g., find online solicitation and sexual extortion message and emails to minors).

For this purpose, the seized laptops and USB sticks are sent to the forensics laboratory for digital forensic investigation.

The above typical use cases highlight several different situations that law enforcement authorities may encounter: (1) either the suspect or victim is present and they or another person are willing and able to provide the necessary information (e.g., PIN code, password, etc.) to access the data, or they are unable to provide the security details necessary for law enforcement authorities to access the data in the seized devices; (2) either the devices are protected by basic, or by advanced, or even by cutting-edge protection; (3) either the devices are typical commercial devices, or devices manufactured and sold for criminal purposes; (4) the type and size of data needed is different depending on the type of investigations conducted.

---

[2] These are chips using the TPM international standard for secure crypto processors (i.e. cryptographic microprocessors).

[3] Bitlocker is an encryption feature in the latest versions of Microsoft Windows operating system that provides entire volumes encryption.

[4] LUKS provides disk encryption.

[5] PGP is an encryption program mainly aiming to increase e0mail communication security.

[6] VeraCrypt is an encryption software that creates virtual encrypted discs.

[7] Peer-To-Peer (P2P) networks are computer networks that the interconnected nodes (peers) share resources without the interference of a centralised administrative system.

Questions:

1. *Do the 3 above use cases summarise correctly the typical situations where law enforcement authorities need to access data at rest in a user's device, or are there other typical use cases that must be considered when assessing challenges relating to data at rest in user's devices?*

2. *In your professional experience, can you estimate the number of cases where you encountered the need to access data at rest in a user's device in the context of a criminal investigation and was it useful to effectively investigate the case?*

3. *Can law enforcement authorities identify the categories of data that might be necessary for the investigation prior to accessing the devices? Is targeted access to these different categories of data always possible?*

4. *Are there specific legal, technical, or operational considerations that should be kept in mind when discussing access to data in the above use cases (for instance regarding rules on applying coercive measures to force a suspect to unlock devices or provide access keys)?*

3. Challenges faced by law enforcement

As set out in the use cases above, electronic devices (laptops, mobile phones, USB keys) can be seized during criminal investigations under judicial supervision. Law enforcement authorities seeking to access data at rest in these devices can face a number of different (possible) challenges, a non-exhaustive list of which is highlighted below:

First, even when a suspect is available to law enforcement authorities to provide access to his/her seized devices, he/she can be unwilling to unlock his/her devices **(Challenge 1).**

Second, modern devices are often encrypted by default[8] to ensure security and confidentiality. In addition, 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 this context, even the most advanced digital forensic tools available to law enforcement authorities are sometimes unable to access and retrieve data from the seized devices in a readable format. **(Challenge 2).**

[8] 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.

Third, even when able to access the device (i.e., the password has either been broken, or provided by the suspect, or the device decrypted), certain files might be protected by robust encryption provided by communication applications such as WhatsApp or Wickr or applications specifically designed to encrypt data such as VeraCrypt. In such cases, law enforcement needs to develop specific bespoke capacities to get access to the data. Not every Member State has the capacity to develop such advanced bespoke capabilities to access encrypted data in a readable format. **(Challenge 3).**

Fourth, some mobile encrypted communication devices (like Encrochat, Sky, etc.) have been specifically designed and marketed for criminal purposes by non-visible companies for criminal use in highly opaque and non-traditional commercial distribution channels. They provide extra layers of encryption guaranteeing perfect anonymity and confidentiality for the user and the phone to be undetectable and untraceable. When law enforcement seizes such devices, they need cutting edge technical capacities to decrypt them, as commercial tools are inefficient. Such expertise might not always be available. **(Challenge 4).**

Fifth, advanced digital forensic solutions used by law enforcement authorities of EU Member States are often developed in third countries, sometimes with a different technological focus and complying with different digital forensic accountability standards than in the EU. **(Challenge 5).**

Questions:

1. *Do you agree that law enforcement authorities of the Member States face the above challenges when having to access data at rest in a user's device? Do all the Member States face them, or some can address these challenges and others not?*

2. *Are there other considerations (technical, legal, other) that law enforcement authorities of the Member States have to take into account when having to access data at rest in a user's device?*

3. *Do you consider that different solutions are required to address these different challenges?*

4. *Would you consider any of these challenges as a priority to remedy for law enforcement authorities? If yes, why?*

5. *Which of these challenges should be further addressed by this working group with the final objective of presenting recommendations for action? Could you already now mention possible solutions to be further analysed in the next meeting of this working group?*