EUROPOL 25

POSITION PAPER ON

Home routing and risks to lawful interception

BACKGROUND

The high security standards and the fragmented and virtualised architecture of 5G standalone will make it harder to carry out lawful interception. This means that law enforcement and judicial authorities are at risk of losing access to valuable data. Already in 2019, the European Council in its ***'Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G'*** stressed the need to address and mitigate potential challenges for law enforcement stemming from the deployment of 5G networks and services[1]. In its position paper on 5G in the same year, Europol outlined challenges pertaining to the availability and accessibility of information needed when conducting lawful interception. In the ***'First report on encryption by the EU Innovation Hub for Internal Security'***, the authors also outline the problems that Home Routing creates for law enforcement agencies in carrying out their duties[2].

OBJECTIVE

The objective of this paper is to highlight to legislatures, national authorities and telecommunication service providers the urgent need to mitigate the challenge that Home Routing poses to lawful interception, as well as present possible avenues for safeguarding and maintaining current investigatory powers.

1 Council of the EU, Significance and security risks of 5G technology – Council adopts conclusions, accessed via: https://www.consilium.europa.eu/en/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/, 2019

2 Europol, First Report on Encryption, accessed via: https://www.europol.europa.eu/publications-events/publications/first-report-encryption, 2024

HOME ROUTING – A SERIOUS CHALLENGE FOR LAWFUL INTERCEPTION

Home Routing makes it possible for a telecommunication service provider to (continue to) provide a service to a customer when they travel abroad. This means that when a customer travels internationally, their communications (calls, messages and data) are still processed through their home network rather than the network of the country they are visiting. This means that the domestic service provider is no longer dependent on the service capabilities of service providers abroad for offering a service to its roaming subscriber. This applies for the services[3] but not for the network access[4], which is provided locally in the visiting country.

Consequently, this means the service provider abroad is **not able to deliver the intercepted communication data in the clear (unencrypted) if the domestic service provider has enabled Privacy Enhancing Technologies (PET) in Home Routing.** For service-level encryption, the subscriber (user) equipment exchanges session-based encryption keys with the service provider in the home network. If PET is enabled, the visiting network no longer has access to the keys used by the home network and therefore data in the clear cannot be retrieved.

Therefore, once Home Routing is deployed, unless a domestic service provider (to whom domestic interception orders can be sent) has a cooperation agreement of not enabling PET in Home Routing in place with the service provider of another country, any suspect using a foreign SIM card can no longer be intercepted. This problem does not only occur when a foreign national uses their own (foreign) SIM card in another country, but **also when citizens or residents use a foreign SIM card in their own country.** Where national law obliges the service providers to deliver the intercepted data to law enforcement agencies (LEAs) in the clear, Home Routing makes it impossible to fulfil this obligation if the home service provider uses service-level encryption. Even if a roaming agreement between the service providers is in place, it creates the problems of:

- LEAs being dependent on the cooperation of the service provider in the country the communication originates from (the home country) and;
- not being able to enforce service providers in the home country (abroad) to adhere to the roaming agreement.

A national interception order cannot be enforced across borders. Instead, a European Investigation Order (EIO) can be issued but a response could take up to 120 days, which is too long in cases where emergency interception is needed. In addition, being dependant on voluntary cooperation between service providers for the exercise of domestic investigatory powers is undesirable.

Example:

Matthew, a suspect in a drug-related offence, who is located in Member State A, buys a SIM card from a Member State B service provider. The MS A authorities learn that he will have a call in two days to discuss the next incoming shipment of cocaine. The MS A authorities order a domestic service provider to intercept his data. The domestic service provider cannot however access the unencrypted data of the service provider abroad, established in MS B, that has supplied the SIM card. The domestic service provider (in MS A) asks the service provider abroad (in MS B) for the unencrypted data on a voluntary basis or as part of a roaming agreement between them. If there is no agreement and no cooperation with the provider abroad, the MS A authorities could send an EIO to the MS B authorities. A response will however most probably not be granted within the necessary two days.

3 Communication services (including voice, video, messaging) are delivered over a standardised architectural framework called the Internet Protocol Multimedia Subsystem (IMS).

4 The process of establishing a connection between the subscriber's device and the network infrastructure (e.g., 4G, 5G), enabling communication and data transfer.

EUROPEAN DIMENSION

The presented challenge is an example of the effect of the European single market, where service providers can operate across borders, but law enforcement capabilities are still limited by their own jurisdictions. The E-evidence regulation (2023/1543)[5], European Investigation Order (2014/41/EU)[6] and the Electronic Communications Code (Directive 2018/1972)[7] make up the European legislation that can be associated with this issue.

The E-evidence instrument **is limited to stored data** and enlarges the jurisdiction of judicial authorities to obtain e-evidence directly from a service provider or its legal representative in another EU Member State.

The European Investigation Order is based on mutual legal assistance and **can take up to 120 days.**

The Electronic Communication Code creates a legal framework to ensure freedom to provide electronic communications networks and services. However, this is without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security, and to permit the investigation, detection and prosecution of criminal offences. In Annex 1 of the Directive, a maximum list of conditions is given, which may be attached to general authorisations. Enabling legal interception by competent national authorities is included in this list.

WAY FORWARD

A solution to the situation described above is urgently necessary. Under Home Routing, the current investigatory powers of public authorities should be retained and a solution must be found that enables lawful interception of suspects within their territory[8]. In addition, an optimal solution should not impede secure communications disproportionately, ensure the confidentiality of criminal investigations, and ultimately enable Member States to execute their legal jurisdictional prerogative to execute investigatory powers. Moving forward, the design and implementation of (new) technologies should be done in the manner that ensure lawful access to data necessary for investigatory powers to carry out their obligations.

5 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543

6 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041

7 https://eur-lex.europa.eu/eli/dir/2018/1972/oj

8 Cross-border interception (interception of suspects outside a Member States' territory) falls outside the scope of this paper.

SOLUTIONS

Feasible solutions aimed at maintaining current investigatory capabilities should be further researched, but they could include some of the following elements:

	1 **Legally mandatory disabling of Privacy Enhancing Technologies (PET) in Home Routing**	2 **Making it possible to request the interception of a suspect's communication in the territory of the requesting Member Sate to a service provider in another Member State**
LEAs operational	This solution maintains the current level of security and law enforcement capabilities. The domestic service provider can execute an interception order for an individual using a SIM card from another country. No target information has to be exchanged with the other country.	This would enable the interception of individuals within MS' own territory. However, the service provider in another Member State would become aware of the person(s) of interest; operationally this might not always be desirable. In addition, it will be very difficult to interpret the data since there is no common interface for supplying/interpreting the data in the EU in the cooperation between law enforcement and service providers. The interface developed for the EIO between law enforcement authorities in different countries could be used, making law enforcement not only dependent on a foreign service provider, but possibly also dependent on enforcement by a foreign authority.
Technical	This solution is technically feasible and easily implemented.	Technically this will require a structural implementation of cross-border standards.
Privacy	The added layer of encryption (PET) is not provided to subscribers abroad in other service provider's networks. Without the additional encryption layer of the home country, **the communication is encrypted at the same level as communication via national SIM cards.** This solution maintains the current level of security, including privacy, and is equal for roamers and local users.	This solution will enable PET for all users.
Policy	National authorities supervising the telecommunication market can enforce an EU regulation mandating the design of the network in this manner.	Failure to comply with the order will require enforcement by the public authority of the Member State where the service provider is established. The E-evidence regulation could serve as an inspiration of how this could be regulated.

POSITION PAPER ON HOME ROUTING AND RISKS TO LAWFUL INTERCEPTION

PDF | ISBN 978-92-95236-32-5 | doi:10.2813/656709 | QL-02-24-737-EN-N

Luxembourg: Publications Office of the European Union, 2024

Cite this publication: Europol (2024), Position Paper on Home Routing and Risks to Lawful Interception, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu