**3GPP TSG-SA WG6 Meeting #69 S6-254357**

**Wuhan, China 13th – 17th Oktober 2025 (revision of S6-254xxx)**

**Source: Netherlands Police**

**Title: Pseudo-CR on Key Issue DM** **Limitations due to regulatory constraints and operator security policies**

**Spec: 3GPP TR 23700-37-030**

**Agenda item: 9.1**

**Document for: Approval**

**Contact: keesdotverweijatpolitiedotnl**

**1. Introduction**

This pCR adds a key issue about how to handle limitations due to regulatory constraints and operator security policies in Discreet monitoring. The text originates from TR 23.784, but has been enhanced as required.

**2. Reason for Change**

This key issue should be addressed in the study.

**3. Proposal**

It is proposed to agree the following changes to 3GPP TR 23700-37-020 v 0.3.0.

\* \* \* First Change \* \* \* \*

## 5.x Key Issue x: Limitations on discreet monitoring due to regulatory constraints and operator security policies

An authorized MC user may request discreet monitoring either on a target MC user or a target MC group. Regulatory constraints and operator security policies can require not to provide media and metadata of transmissions from MC service users who are communicating with the discreet listening target MC service user, and who are not themselves targets of discreet listening.

Issues:

- How only the communication transmissions coming from the target MC user involved in a private communication can be part of discreet monitoring.

- How only the communication transmissions coming from one target MC user involved in a group communication can be part of discreet monitoring.

- In a group regrouping scenario of a target MC group: How only the communication transmissions coming from members affiliated to the target MC group can be part of discreet monitoring.

- How communication transmissions from non-target participant(s) are made unavailable to the authorized MC user, as they are not part of discreet monitoring requests.

- Whether parts of the metadata of the transmissions of non-target participant(s) should be provided to the authorized user to provide context to the communications of the target user without violating the regulatory constraints and operator security policies.\* \* \* End of Changes \* \* \* \*