**3GPP TSG-SA3 Meeting #124 draft\_S3-253177-r3**

**Wuhan, China, 13th - 17th October 2025**

**Source: ZTE, NTT DOCOMO(?)**

**Title: New key issue on privacy protection for sensing service**

**Document for: Approval**

**Agenda item: 5.2.7**

**Spec: 3GPP TR 33.777**

**Version: 0.1.0**

**Work Item: FS\_Sensing\_SEC**

**Comments**

This contribution proposes a new key issue about privacy protection for sensing service.

**Proposed Changes**

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

## 5.X Key Issue #X: Privacy protection for sensing service

### 5.X.1 Key issue details

The introduction of sensing capabilities enables the network to collect and process sensing data about objects in the environment and expose derived sensing results, all without the direct participation or awareness of the sensed object. Considering that the sensing data or sensing result can contain privacy sensitive information, the privacy aspect of sensing service needs to be investigated.

### 5.X.2 Security threats

If the sensing data contains privacy related information, then that information could be leaked to undesired party, leading to privacy violation.

### 5.X.3 Potential security requirements

The 5G system shall provide a mechanism to mitigate privacy threats.

NOTE x: For aerial object (e.g., UAV) detection and tracking use case, the above security requirement is not applicable.

NOTE y: The security requirement do not require 3GPP to provide mechanism(s), as this can be addressed by out-of-3GPP, e.g., Regulations.

\* \* \* End of Changes \* \* \* \*