KHAITAN &CO ADVOCATES SINCE 1911

UPDATE

ERGO

Analysing developments impacting business

NEW RULES FOR LAWFUL INTERCEPTION OF TELECOMMUNICATIONS

11 September 2024

The Department of Telecommunications (DoT), on 28 August 2024 released the draft Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 (Rules). The Rules are slated to be taken into consideration after expiry of 30 days from the date of its publication in the Official Gazette. In the meantime, interested stakeholders can submit observations and suggestions in respect of the Rules.

Issued in supersession of rules 419 and 419A of the Indian Telegraph Rules, 1951 (collectively, Existing Rules), the Rules lay down the procedure and safeguards for authorized entities to conduct lawful interception of messages in telecommunication under the Telecommunication Act, 2023 (Telecom Act).

Background

Under Section 20 of the Telecom Act, authorized agencies of the Central Government or State Government can intercept or receive any message or class of messages pursuant to an interception order. Such interception orders can be passed upon the occurrence of any public emergency or in the interest of public safety, when the relevant authorised agency is satisfied that it is expedient to do so in the interest of national security and interest. Orders can also be passed for restricting the transmission of certain messages. Given that orders of this nature are likely to impinge upon the personal liability and privacy of individuals as well as impact 'telecommunication entities' (i.e., entities that provide telecom services and establish, operate, maintain and expand telecom networks, including entities that are authorised or exempted under the Telecom Act (Telecom Entity)), there is a need to lay down checks and balances to prevent misuse.

Key provisions of the Rules

- *Procedure for interception of messages by authorized agencies*:
    - The Central Government may by order specify one or more authorized agencies to intercept or receive messages or class of messages pursuant to an interception order passed under the Telecom Act.
    - Interception orders for directing interception of messages may be passed by the 'competent authority', i.e., the Union Home Secretary of the Ministry of Home Affairs (in case of the Central Government) or Secretary to the State Government in charge of the Home Department (in case of a State Government).
    - All interception orders issued by the 'competent authority' shall be submitted to the relevant review committee (Review Committee) of the Central or State Government, within a period of 7 working days. It is also necessary that the relevant authority should have ensured that it would not be possible to acquire the necessary information by any other reasonable means.

  - In unavoidable circumstances, interception orders may be passed by an authorized officer not below the rank of a Joint Secretary to the Central Government. Further, in emergent cases in remote areas or for operational reasons, where it is not feasible for the 'competent authority' to issue an interception order, the Rules prescribe an alternate procedure that can be followed. In such cases, the interception order may be issued by the 'head' or second senior most officer not below the rank of Inspector General of Police of an authorized agency, subject to certain processes and safeguards. It is also necessary to submit the order to the designated 'competent authority' for its confirmation, failing which the interception cannot take place.

- *Constituents of interception order*: The Rules prescribe the information that must be stipulated in the interception order. This includes the name of the authorized agency that will undertake the interception, reasons for undertaking interception and the period (subject to a maximum of 60 calendar days, and extendable to 180 days in certain cases) for which the interception order shall remain in force.

- *Record keeping*: According to the Rules, the relevant authorized agency undertaking interception pursuant to an interception order must maintain secure records as prescribed. This includes records of the intercepted messages, particulars of the person whose messages were intercepted, name and particulars of the officer to whom intercepted messages were disclosed, number of copies made, date of destruction of copies, etc. Such records are required to be deleted every 6 months, unless required for functional requirements. DoT is also required to destroy such records within 2 months of discontinuance of the interception in a particular case.

- *Implementation of an interception order*: For implementing an interception order passed pursuant to the established process, 2 nodal officers each are required to be appointed by the authorized agency, DoT and Telecom Entity (note that DoT and Telecom Entity must appoint 2 nodal officers in every telecom service area). No other officers are permitted to handle matters relating to an interception order. Additionally, adequate and effective safeguards must be implemented to prevent unauthorized interception of messages and ensure that confidentiality and secrecy is maintained. Timelines have also been prescribed for nodal officers of DoT and Telecom Entity to acknowledge the interception orders and submit fortnightly reports to the authorized agency that issued it.

- *Constitution of Review Committee*: The Rules envisage that Review Committees will be constituted at a Central and State level. Such Review Committees, comprising of senior bureaucrats from the Government, will be entrusted with ensuring that interception orders are passed in accordance with the Telecom Act and the Rules. The relevant Review Committee may set aside an interception order, order destruction of copies of intercepted messages in case it is of the opinion that the interception order does not meet the conditions.

Comment

The Rules are aimed at ensuring that interception of messages does not take place in any unlawful manner, by proposing a system of checks and balances. In comparison to the Existing Rules, the Rules do not seek to overhaul the framework relating to lawful interception of messages. Most requirements from the Existing Rules, barring certain deviations in terms of designations of officers, have found their way to the Rules. Given the broader definition of Telecom Entities under the scope of the Rules, it will be important to monitor how the Rules are implemented upon coming into effect.

As the awareness around data privacy grows and cyber attacks become more sophisticated, it remains to be seen whether the procedural safeguards and measures outlined in the Rules strike a desirable balance between surveillance and privacy rights.

- *Harsh Walia (Partner); Shobhit Chandra (Counsel); Sanjuktha A. Yermal (Senior Associate) and Vanshika Lal (Associate)*

For any queries please contact: editors@khaitanco.com