GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

RAJYA SABHA
UNSTARRED QUESTION NO. 21
ANSWERED ON 29TH JANUARY, 2026

DATA PRIVACY FOR SANCHAR SAATHI APP

21   DR. JOHN BRITTAS:

Will the Minister of Communications be pleased to state:

(a)   the number of downloads of Sanchar Saathi application since its launch, State-wise and year-wise;

(b)   the number of complaints registered through the application and resolved, State-wise;

(c)   the nature and extent of user data collected through the application, including metadata, device information and SIM-related details;

(d)   whether any personal or usage data, collected through Sanchar Saathi, is shared with other Government agencies or third parties;

(e)   if so, the details thereof; and

(f)   whether any independent audit or privacy impact assessment has been conducted prior to or after large-scale deployment of the application?

<div align="center">ANSWER</div>

<div align="center">MINISTER OF STATE FOR COMMUNICATIONS AND RURAL DEVELOPMENT
(DR. PEMMASANI CHANDRA SEKHAR)</div>

(a)   Sanchar Saathi mobile App has 1.77 crore downloads since its launch on 17.01.2025. State wise data of downloads is not maintained.

(b)   Sanchar Saathi initiative can be accessed by citizens through web portal (www.sancharsaathi.gov.in) as well as mobile App. Based on the requests submitted by the citizens on the Sanchar Saathi, following actions have been taken:

   i. 27.96 lakh lost/ stolen mobile handsets have been traced and 8.22 lakh lost/ stolen mobile handsets have been recovered and returned to rightful owners by State/ UT Police.
   ii. 2.22 crore mobile connections have been disconnected based on reporting by citizens as 'Not My Number' or 'Not Required'.
   iii. 39.42 lakh mobile connections have been disconnected based on 7.72 lakh inputs provided by vigilant citizens related to suspected fraud communications.

Detailed statistics have been made available on the Sanchar Saathi portal for citizens.

(c) to (e)   Sanchar Saathi App follows a permission-based data minimization approach. App requires users to do necessary registration, informs users about the data that is essential for each feature, and takes due permissions from the users, thus taking care of user's consent. The app does not have access to any sensitive personal information like contacts, location, microphone, Bluetooth, other apps, or any other private functionalities/data of the user that is specifically not permitted by the user while using the App. Further, citizens have choice to remove any permission any time or deregister any mobile number registered on the App and also to uninstall the App.

(f)   The App has been allowed to be hosted on Android and iOS platforms only after due security and vulnerabilities assessments. Periodic third-party security audit of the App is conducted by certified auditor.

*****