

Sanchar Saathi App: Features, Mandate, Privacy Issues & Govt Rules Explained

December 3, 2025 • vajiramandravi.com



Sanchar Saathi Latest News

- The Centre has directed smartphone manufacturers to **preinstall** the government-developed **Sanchar Saathi** app on all new devices and push it via software updates to existing phones.
- The app allows users to report fraudulent calls, scam messages, and stolen mobile phones. Importantly, the government has asked that the app cannot be deleted by users.
- Earlier, the DoT told companies that the app must be non-deletable, non-restrictable, and non-disableable, raising concerns about privacy and forced compliance.
- Later, the Telecom Minister clarified that Sanchar Saathi is not mandatory and users may delete it if they wish.

About Sanchar Saathi

- Sanchar Saathi is an optional mobile app and website developed by the Department of Telecommunications (DoT).
- It aims to **empower** mobile users, enhance security, and raise awareness about government initiatives.
- The platform provides multiple citizen-focused services, along with updates and educational material on telecom, cybersecurity, and end-user protection.

Key Services Offered by Sanchar Saathi

- Sanchar Saathi provides a range of tools to strengthen user security, prevent fraud, and help track stolen devices.

Chakshu: Reporting Suspected Fraud Communication

- Chakshu allows users to report suspicious calls, SMS, WhatsApp messages, or other communications linked to:
 - Impersonation of DoT, TRAI, police, or government officials
 - Investment or trading scams
 - Fake KYC or payment-related messages from banks, utilities, or insurance
 - Malicious links, phishing attempts, unverified APKs, and device-cloning attempts
- Chakshu **cannot** be used to file cybercrime complaints.
- Users may also report spam or Unsolicited Commercial Communication (UCC), which is addressed under The Telecom Commercial Communication Customer Preference Regulation (TCCCPR), 2018 regulations of TRAI.

Block and Track Lost or Stolen Mobile Phones

- Sanchar Saathi enables users to:
 - Block a lost or stolen mobile device
 - Trace the device when someone tries to use it
 - Unblock it after recovery
- The service uses the phone's IMEI number, a unique 15-digit identifier stored by mobile networks.

Mandatory Phone-Number Registration

- Registration using a mobile number is compulsory for using the app's features.
- The app states this is required to "identify the mobile number" linked to its services.
- On Android phones, the app automatically detects the active phone number and sends a registration SMS to DoT without explicit user consent.
 - This has raised major privacy concerns.

What Permissions Sanchar Saathi Seeks on Android

- **Send SMS** – Enables the app to send the automatic registration SMS to DoT.
- **Call and SMS Logs** – Allows reporting suspicious calls or messages through the app.

- **Photos and Files** – Needed to upload screenshots of scam calls/SMS or documentation for lost/stolen phone reporting.
- **Camera Access** – Used to scan a phone's IMEI barcode to verify device authenticity.

Legal Basis for Mandating Sanchar Saathi

- The government's directive relies on expanded powers under the **Telecommunications Act, 2023** and the amended **Telecom Cyber Security (TCS) Rules, 2024**.
 - TCS rules were amended in 2025.
- While DoT had earlier assured that its mandate would remain limited to telecom operators, the November 2025 amendment broadened the scope significantly.

Expanded Definition: Who Falls Under DoT's Authority Now

- The amendment introduced the term **Telecommunication Identifier User Entity (TIUE)** — covering any entity that uses a phone number to identify users.
- This includes:
 - Smartphone manufacturers
 - Messaging platforms like WhatsApp
 - Apps requiring phone-number verification
- Under this broadened definition, DoT:
 - Mandated WhatsApp and other platforms to auto-log-out web sessions every six hours
 - Required WhatsApp accounts to stop working if used on devices without the registered SIM
- The Sanchar Saathi pre-installation mandate arises from this expanded rule set.

Constitutional Concerns and Right to Privacy

- Experts warn that forced installation and a ban on uninstalling the app may face constitutional scrutiny.
 - Smartphone makers warn that complying with the mandate may require deep OS-level changes, potentially weakening device security.
 - Concerns are amplified because:
 - Sanchar Saathi is government-backed, and state agencies receive broad exemptions under India's **Data Protection Act**.
 - Critics fear this could give the Centre greater control over digital ecosystems and expand state surveillance capabilities.
- Experts noted:
 - The **Puttaswamy judgment** protects the right to privacy.
 - State-mandated apps must meet tests of legality, necessity, proportionality, and least intrusive means.
 - Aadhaar survived scrutiny partly because it was categorised as **voluntary** at the time.
- By making Sanchar Saathi pre-installed and uninstalleable, the mandate shifts from a voluntary security tool to compelled compliance, raising privacy concerns.

Source: <https://vajiramandravi.com/current-affairs/sanchar-saathi-app-features-mandate-privacy-issues-govt-rules-explained/>

© Vajiram & Ravi. For personal use only.