GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *313
TO BE ANSWERED ON: 28.03.2025

MEASURES TO PREVENT MISUSE OF PERSONAL DATA

***313. SHRI SADANAND MHALU SHET TANAVADE:**

Will the Minister of ELECTRONICS & INFORMATION TECHNOLOGY be pleased to state:-

(a) whether the Ministry is aware that citizens are frequently receiving unsolicited phone calls from unknown individuals and companies engaging in cold-calling to sell products and services, thereby intruding upon their privacy;
(b) whether Government is aware of the misuse and unauthorized sale of citizen's personal data to third parties;
(c) if so, the steps taken by the Ministry to curb such practices; and
(d) whether Government has formulated or plans to formulate measures to protect citizens from datamisuse and fraud, and to prevent the unauthorized extraction, misuse, and sale of personal data; if so, the details thereof?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (d): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *313 FOR 28.03.2025 REGARDING MEASURES TO PREVENT MISUSE OF PERSONAL DATA

……

(a) to (d):Unsolicited Commercial Communications (UCC) are regulated by the Telecom Regulatory Authority of India (TRAI). TRAI has issued Telecommunications Commercial Communications Consumers Preference Regulations, 2018 (TCCCPR-2018) which deals with UCC.

Under the TCCCPR-2018 regulations a number of directions have been issued for the implementation of its provisions. These directions inter-alia have provisions for registering preferences for commercial communication where a telecom subscriber can opt to block all commercial communications or can selectively block commercial communications as per preference categories.

Customers can register complaint against senders of UCC through Mobile App, sending SMS or calling on a specific number 1909.

The Government of India has taken major initiatives like enactment of Information Technology (IT) Act, 2000, setting up of Indian Computer Emergency Response Team and National Critical Information Infrastructure Protection Centre, releasing of National Cyber Security Policy 2013, appointing Chief Information Security Officer, thus ensuring security and privacy of personal information of users in India.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under the IT Act prescribes reasonable security practices and procedures to protect sensitive personal data of users.

Digital Personal Data Protection Act, 2023 ("DPDP Act") provides the legal framework for processing of personal data, notice to be issued to data principal, consent of the data principal including withdrawal of such consent, rights of the data principal, obligations of the data fiduciaries, penalties for non-compliance, etc.

The DPDP Act provides legal framework for Data Fiduciaries to notify breaches and ensure effective observance of the provisions Act by implementing appropriate technical and organizational measures.

Further, the DPDP Act establishes a robust framework of accountability mechanisms to ensure the lawful processing of digital personal data with Data Protection Board of India as an independent adjudicatory body empowered to investigate complaints, conduct inquiries, and impose penalties.

Ministry of Home Affairs has also established the Indian Cyber Crime Coordination Centre to deal with cyber-crimes in a comprehensive and coordinated manner.

Public awareness campaigns, such as Cyber Security Awareness Month and Safer Internet Day, are organized to educate citizens about online safety, secure online transactions and digital services.

****