GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 2460
TO BE ANSWERED ON: 21.03.2025

PLANS TO ADDRESS UNAUTHORIZED DATA ACCESS

2460. SHRI VIVEK K. TANKHA:

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

(a) whether there has been an increase in privacy breaches, particularly due to inadequate enforcement and surveillance practices despite the introduction of the Digital Personal Data Protection Act;
(b) the manner in which Government plans to address unauthorized data access and ensure stronger protection;
(c) the concrete steps Government will take to tackle this growing issue and protect citizens from personal data theft and cybercrimes; and
(d) whether Government intend to implement stricter laws and enforcement measures to prevent identity theft and secure personal data with personal data becoming increasingly vulnerable?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): The policies of Government of India are aimed at ensuring an open, safe, trusted and accountable cyberspace for users in the country. Government of India has taken major initiatives like enactment of Information Technology (IT) Act, 2000, setting up of Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC), releasing of National Cyber Security Policy 2013, appointing Chief Information Security Officer (CISO), thus ensuring protection of personal data of users in India.

The Information Technology Act, 2000 ("IT Act") contains several offences and penalizes different categories of cybercrime such as tampering with computer source documents, identity theft, cheating by impersonation, violation of privacy, publishing or transmitting obscene material, depicting sexually explicit material including children. The Bhartiya Nyay Sanhita (BNS) also addresses cybercrime specifically targeting cyberbullying, identity theft, and online harassment, ensuring stricter penalties for such offenses. It also tackles fraudulent online transactions, cyberstalking, and data breaches, aiming to protect personal and financial information.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 made under section 43A of the IT Act prescribes reasonable security practices and procedures and sensitive personal data or information to protect sensitive personal data of users. These include the requirement that any person collecting, receiving, possessing, storing or dealing information should publish on its website a privacy policy and disclosure of personal information, that such person use the information collected for the purpose for which it was collected and keep it secure, that disclosure of sensitive personal data be done with prior permission of the information provider, that sensitive personal data or information not be published, and that a third party receiving sensitive personal data or information shall not disclose it further. Additionally, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 made in exercise of the powers given under the IT Act obligates intermediaries,

including social media intermediaries, to prevent users from hosting, displaying, uploading, or sharing content that belongs to another person and to which the user does not have any right and they have to implement measures to ensure data protection and prevent unauthorized data access.

Also, the Digital Personal Data Protection Act, 2023 ("DPDP Act") obligates organizations involved in digital personal data processing, to implement robust compliance measures, including obtaining consent for specified purposes before lawful processing of digital personal data and respect for individual rights. The Act requires Data Fiduciaries to process personal data responsibly, notify breaches promptly, and ensure effective observance of the provisions of the 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 of up to ₹250 crore for non-compliance of the provisions of the Act.

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. The cyber security advisories are regularly issued on emerging threats, mitigation strategies, and best practices to safeguard data. Initiatives like the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) and the National Cyber Coordination Centre (NCCC) focus on detecting and mitigating malicious activities, enabling situational awareness, and securing against potential threats.

******