GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**RAJYA SABHA**
**UNSTARRED QUESTION NO. 3261**
TO BE ANSWERED ON: 20.03.2026

**UNAUTHORIZED ACCESS TO MAJOR NATIONAL DIGITAL INITIATIVES BY PRIVATE CITIZENS**

**3261. SHRI JAVED ALI KHAN:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether the Ministry has conducted any internal review or sought a report on instances of private citizens' access to major national digital initiatives and propagating specific elements of a major national digital initiative abroad with unauthorized persons before the launch of the schemes;
(b) if so, whether any protocol or guidelines exist in the Ministry to prevent premature disclosure of forthcoming Government flagship programmes to foreign entities or individuals;
(c) if so, the details thereof and if not, reasons therefor; and
(d) the steps taken or proposed to be taken by the Ministry to ensure that no sensitive policy information is compromised?

**ANSWER**

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

(a) to (d): The Government accords high priority to safeguarding sensitive policy information and ensuring responsible handling of digital data.

The policies of Government of India are aimed at ensuring open, safe, trusted and accountable cyberspace for all users and the Government has instituted a comprehensive legal and regulatory framework to address cyber-enabled crimes and to promote a safe, trusted, and accountable digital ecosystem.

The Government has taken several steps to strengthen the framework for digital services and data protection in the country.

The Information Technology Act, 2000 ("IT Act") and the rules made thereunder provide for penal action against a wide range of cyber offences, including computer-related offences, cybersecurity breaches, impersonation, identity theft, violation of privacy, circulation of obscene content, and child sexual abuse material.

The IT Act penalises various cyber offences relating to computer resources, including dishonestly or fraudulently accessing a computer resource without the permission of its owner, commonly referred to as hacking (section 66), or making an attempt to unauthorised access to a protected system (CII) (section 70).

The Digital Personal Data Protection Act, 2023 ("Act"), and the Digital Personal Data Protection Rules, 2025 ("Rules"), were notified on 13 November 2025. The Act provides for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.

The Act is technology agnostic and has been intentionally structured with flexibility to accommodate evolving digital technologies. It provides a comprehensive framework for the

protection of digital personal data and ensures accountability of Data Fiduciaries in respect of personal data breaches.

In addition, the Government has comprehensive protocols and legal frameworks in place to prevent the premature or unauthorised disclosure of sensitive information regarding flagship programmes.

These include provisions under the Official Secrets Act, 1923, which prohibits unauthorised communication of official information, and the Central Civil Services (Conduct) Rules, 1964, which require government servants to maintain integrity, confidentiality and devotion to duty. Further, the Manual of Office Procedure prescribes detailed procedures regarding handling, classification (Top Secret, Secret, Confidential) and safeguarding of official documents and records, including restrictions on disclosure of sensitive information.

Ministries/departments are required to follow established Government procedures and applicable rules relating to information security, confidentiality of official records, and dissemination of policy information.

Further, the provisions of the Right to Information Act, 2005 provide exemptions from disclosure of certain categories of information, including those covered under Sections 8(1)(a), 8(1)(c), and 8(1)(i) relating to national interests, breach of privilege of Parliament/State Legislature, and Cabinet papers, respectively.

These procedures ensure that policy proposals, draft documents and other sensitive information are handled with due confidentiality until formally approved and placed in the public domain.

******