

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2297
TO BE ANSWERED ON: 07.08.2026

VERIFICATION OF MOBILE APPLICATIONS AND CYBERSECURITY

2297. SHRI BABUBHAI JESANGBHAI DESAI:

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

- (a) whether Government has taken note of the growing practice of app stores and digital platforms requiring verification of applications and developers prior to publication;
- (b) if so, the reasons therefor and the security, privacy and consumer protection objectives sought to be achieved through such verification;
- (c) whether Government has prescribed any standards or guidelines for App verification, user data protection and detection of malicious applications; and
- (d) the steps taken to strengthen cybersecurity and safeguard users from fraudulent, harmful or misleading mobile applications?

ANSWER

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

(a) to (d): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. The existing legal framework including the Information Technology Act, 2000 ("IT Act") and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules"), together, have put in place a framework to deal with unlawful and harmful content in the digital space and impose clear obligations on intermediaries to ensure accountability. The IT Rules require that the app stores as an intermediary shall:-

- observe due diligence while discharging their duties and shall inform the users of computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is misleading, unlawful or violates any law for the time being in force.
- take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 ("SPDI Rules").
- take all reasonable measures to ensure accessibility of its services to users along with reasonable expectation of due diligence, privacy and transparency.

The SPDI Rules require organisations including digital platforms to collect personal data only for stated purposes, obtain consent before sharing it, and publish privacy policies. Sensitive personal data must not be published and must not be further disclosed by third parties.

The Government enacted the Digital Personal Data Protection Act, 2023 (“DPDP Act”), which establishes a comprehensive framework for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes. The DPDP Act also establishes strong transparency and accountability obligations for organisations that process digital personal data. Entities that determine the purpose and means of processing such data, referred to as Data Fiduciaries, must provide clear notice to individuals about the personal data being collected, the purpose for which it will be processed, and the manner in which individuals may exercise their rights.

On 10th February, 2026, the Government strengthened the regulatory framework by including reduced timelines for removal or disabling access of unlawful information by intermediaries upon actual knowledge including valid reasoned intimation from the Appropriate Government or court orders (timeline reduced from 36 hours to 3 hours).

Social media intermediaries having more than 50 lakh registered users in India (Significant Social Media Intermediaries) are required to enable their users to voluntarily verify their accounts and provide such accounts with visible marks of verification. It must be ensured that the information received for the purpose of verification shall not be used for any other purpose unless the user expressly consents to it.

The Government has institutionalised a nationwide integrated and coordinated framework to strengthen cybersecurity and digital resilience across digital ecosystems, which, inter alia, includes:

- National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination related to cyber security amongst different agencies.
- The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the IT Act.
 - o CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis. CERT-In coordinates appropriate remedial measures with service providers in cases of malware affecting mobile devices.
 - o CERT-In has issued Guidelines for Secure Application Design, Development, Implementation & Operations” for the entities engaged in developing or outsourcing application development.
- National Cyber Coordination Centre (NCCC), implemented by CERT-In, examines cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.
- The Government has established the National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country under the provisions of section 70A of the IT Act.

- The Consumer Protection Act, 2019, administered by the Department of Consumer Affairs, Ministry of Consumer Affairs, Food and Public Distribution, was enacted to modernize the framework governing consumer protection in the era of globalization, technologies, e-commerce markets, etc.
- ‘Information Security Education and Awareness (ISEA)’ project is implemented by MeitY for strengthening human resources in the area of Information Security and creating general awareness. Awareness material on various aspects of cyber hygiene & cyber security is disseminated through portals such as www.staysafeonline.in, www.infosecawareness.in and www.csk.gov.in.
