GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 2389**
TO BE ANSWERED ON: 21/12/2022

## LEAKAGE OF PERSONAL AND PRIVATE DATA

**2389. SHRI SUNIL DATTATRAY TATKARE:**
**SHRIMATI SUPRIYA SULE:**
**DR. SUBHASH RAMRAO BHAMRE:**
**DR. AMOL RAMSING KOLHE:**
**SHRI KULDEEP RAI SHARMA:**

Will the Minister of Electronics and Information Technology be pleased to state:

(a) the total number of cases where Indians' Personal and Private data has been allegedly got leaked or shared by Social Media companies, Private entities, Government or any other organization, institution or body since 2015 without people consent;
(b) the actions taken by the concerned authorities in every individual case alongwith the remedies provided to people, if any;
(c) whether any compensation was given by the Government to the victims of these cases and if so, the details thereof;
(d) whether the Government has any direction to the companies to take steps for protection of the user data and if so, the details thereof and if not, the reasons therefor;
(e) whether the Government can collect, use and share personal information of people in any way they desire without asking for consent; and
(f) if so, the extent to which the Government legally is immune to collect, share and use in any way they desire, the personal information of people without their explicit consent?

## ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The cyber space is anonymous and borderless and has become very sophisticated and complex with the technological innovations and inclusion of different type of devices and services. Any data breach of Indian users is required to be reported to the Indian Computer Emergency Response Team (CERT-In), which is the national nodal agency for incident response in the country and for the collecting information on cyber incidents. As per the information reported to and tracked by CERT-In, a total of 14, 6 and 22 incidents were reported during the years from 2020, 2021 and 2022 (up to November) respectively.

(b): On observing data leakage or breach, CERT-In notified the affected organisations along with remedial actions to be taken. CERT-In coordinated incident response measures with affected organisations, service providers and respective sector regulators as well. Further, to educate people and organisations, CERT-In has also issued alerts and advisories on an ongoing basis regarding latest cyber-threats/vulnerabilities and countermeasures.

(c) and (d): Section 43A of the Information Technology Act, 2000 ("IT Act") provides that a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, causing wrongful loss or wrongful gain to any person on account of its negligence in implementing and maintaining reasonable

security practices and procedures is liable to pay damages by way of compensation to the affected person. The Government, in exercise of its powers under the said section, has made the Information Technology (Reasonable Security Practices and Procedures and Sensitive

Personal Data or Information) Rules, 2011 (SPDI Rules), prescribing the security practices and procedures that a body corporate or any person collecting, receiving, possessing, storing, dealing or handling information on behalf of such body corporate is required to observe for protecting personal data of users. These include the requirements that such body corporate or person publish on the website a policy for privacy and disclosure of personal information, data or information, use the information collected for the purpose for which it was collected, keep it secure, and obtain prior permission of the information provider for disclosing sensitive personal data. On violation of these rules, an aggrieved person can approach the adjudicating officer under the IT Act for compensation. Government has appointed the Secretary of the Department of Information Technology of each State and Union territory as the adjudicating officer for this purpose. Government does not maintain a record of compensation given to victims.

Further, section 72A of the IT Act provides for punishment for disclosure of information in breach of lawful contract.

The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs has been designated as the nodal point in the fight against cybercrime. A toll-free number 1930 has been made operational for citizens to get assistance in lodging online complaints in their own language. To spread awareness on cybercrime, the Ministry of Home Affairs has taken several steps that include dissemination of messages on cybercrime through the Twitter handle @cyberDost and radio campaigns.

In addition to the above, the following measures have been taken to enhance the cyber security posture and prevent data leaks:

(i) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.
(ii) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.
(iii) CERT-In has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.
(iv) CERT-In conducts regular training programmes for network and system administrators and the Chief Information Security Officers of government and critical sector organisations regarding securing the information technology infrastructure and mitigating cyber-attacks.
(v) All government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting as well.
(vi) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.
(vii) CERT-In operates an automated cyber-threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
(viii) Cyber security mock drills are being conducted to enable assessment of cyber security posture and preparedness of organisations in the government and critical sectors.
(ix) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

(x) CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites.
(xi) The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Specific books, videos and online materials

are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

(e) and (f): No sir/madam. Legal requirement regarding collection, use and sharing of personal information by a person, including the Government, arises from various laws for the time being in force, and any relevant binding judicial decisions.

The SPDI Rules, 2011 requires a body corporate to obtain prior permission of the information provider for disclosing sensitive personal data, unless such disclosure has been contractually agreed to between the body corporate and the information provider, or it is necessary for compliance of a legal obligation, or the information is to be shared with Government agencies mandated under the law to obtain information for the purpose of verification of identity or prevention, detection, investigation, prosecution and punishment of offences.

Further, the Ministry of Electronics and Information Technology has prepared a draft Bill, titled the Digital Personal Data Protection Bill, 2022 and has invited feedback from the public as part of its public consultation exercise. The draft Bill sets out the rights and duties of the citizen (Digital Nagrik) and the obligations of the Data Fiduciary to use the collected data lawfully.

*******