

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**LOK SABHA**  
**UNSTARRED QUESTION NO.1630**  
TO BE ANSWERED ON: 13.02.2019

**BREACH OF DATA BY SOCIAL MEDIA SITES**

**1630**            **SHRI PARVESH SAHIB SINGH:**  
**SHRI PRALHAD JOSHI:**

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

- (a) whether the Government has noted any cases of data breach by private social media websites operating in India, if so, the details thereof;
- (b) whether the Government has recently asked the social networking firm Facebook to provide India specific details on the company's latest security breach and if so, the details thereof and response thereto;
- (c) the details of disciplinary actions taken by the Government against any social media website operators for not complying with cyber laws in India within the last four years;
- (d) whether the Government finds existing cyber laws in India adequate for ensuring data privacy in India and if so, the reasons therefor; and
- (e) if not, whether it plans to strengthen it and if so, the plan of action in this regard?

**ANSWER**

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY  
(SHRI S.S. AHLUWALIA)

(a), (b) and (c): Yes, Sir. Few instances of data breaches by private social media websites were reported in the media. Government took notice of reports about leakage of data by Facebook and Cambridge Analytica, and in responses to notices sent to them, Facebook conveyed that there had been unauthorised data leakage by Cambridge Analytica. However, since the reply given by Cambridge Analytica was not adequately convincing, CBI has been asked to investigate this matter with regard to possible misuse by Cambridge Analytica.

In addition, one incident of breach of personal data of Indian users from a social media company was reported to the Indian Computer Emergency Response Team (CERT-In). As per information available external actors exploited vulnerability in the form of software bugs impacting a feature provided for users on a social media platform. This allowed unauthorised access to users' account and information. The Indian Computer Emergency Response Team (CERT-In) issued advisories to users regarding best practices to be followed for protection of account information while using Social Media.

(d) and (e): The cyber world is dynamic, evolving in nature and is fast changing. Section 43A and section 72A of the Information Technology Act, 2000 provides for privacy and security of data in digital form. Section 43A provides for compensation to be paid to the victim in case of unauthorized access of information and leakage of sensitive personal information respectively. It mandates 'body corporates' to implement 'reasonable security practices' for protecting 'sensitive personal information' of individuals. Section 72A of the Act provides for punishment for disclosure of information in breach of the lawful contract. Further, Information Technology (Intermediary Guidelines) Rules 2011 notified under Section 79 of the IT Act, 2000 require that the Intermediaries shall observe due diligence while discharging their duties and shall publish the rules and regulations, privacy policy and user agreement for access or usage of its computer resource by any person.

To further strengthen personal data protection of user, Government had set up a Committee of Experts under the Chairmanship of Justice (Retd.) Shri B N Srikrishna to prepare a data protection framework and work out the Data Protection Bill. The Srikrishna Committee deliberated on various issues and brought out a White Paper on Data Protection that laid down the principles. Thereafter, the Committee submitted its report along with draft Bill to MeitY. The report and the draft Bill were placed in the public domain and comments were sought. Feedback has been received and based on the analysis of the feedback received certain modifications in the Bill are being carried out and steps are afoot to bring about data protection legislation.

\*\*\*\*\*