GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2470
TO BE ANSWERED ON: 01.08.2018

PROTECTION OF PRIVACY OF CITIZEN

2470 . SHRI B.V. NAIK:

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

(a) whether the Government protects the privacy of citizens on internet and if so, the details of steps taken in this regard;

(b) whether the Government has allowed private entities, Indian and foreign, to access personal data of individuals stored under Aadhaar and other Government sponsored schemes;

(c) if so, the details thereof and the reasons therefor; and

(d) whether the Government will make arrangements to protect/secure the vast data of the public under the purview of Government?

ANSWER

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

(a): Yes, Sir. Section 43, section 43A and section 72A of the Information Technology Act, 2000 provide for privacy and security of data in digital form. Further, Government is considering bringing data protection legislation in the country. A Committee of Experts on Data Protection chaired by Justice Shri. B.N Srikrishna (Retd.) had been constituted to look into the aspects pertaining to Data Protection. The Committee has submitted its report along with draft Bill to Government on 27th July, 2018.

(b) and (c): UIDAI provides demographic information (limited/full) as a part of eKYC services to authorised and approved entities as per the provisions of Aadhaar Act, 2016 and Regulations framed thereunder.

(d): In respect of UIDAI, it is informed that UIDAI has a well-designed, multi-layered robust security system in place and the same is being constantly upgraded to maintain the highest level of data security and integrity. UIDAI has adequate legal, organizational and technological measures in place for the security of the data stored with UIDAI. Data Protection measures have also been mandated for the requesting entities and ecosystem partners to ensure the security of data. Government is fully alive to the need to maintain highest level of data security, privacy and is deploying the necessary technology and infrastructure. The architecture of Aadhaar ecosystem has been designed to ensure non-duplication, data integrity and other related management aspects of security & privacy in

Aadhaar database. Additionally, various policies and procedures have been defined clearly which are reviewed and updated periodically, thereby, appropriately controlling and monitoring security of data.

There are multiple layers of security at physical level in UIDAI Data Centres and is being managed by armed CISF personnel round the clock. Strengthening of security of data is an ongoing process and all possible steps are being taken in this regard. Further, Chapter VI (Protection of Information) of The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ("The Aadhaar Act") and the AADHAAR (DATA SECURITY) REGULATIONS, 2016 framed there under have been specifically drafted keeping in account the various security requirements in respect of data collected by UIDAI.

Security Audits are conducted on regular basis by Standardisation Testing and Quality Certification (STQC) Directorate, which is an attached office of the Ministry of Electronics and Information Technology, Government of India. UIDAI has been declared ISO 27001:2013 certified by STQC with respect to Information Security which has added another layer of information security assurance. Further in pursuance of sub-section (1) of Section 70 of the IT Act 2000, UIDAI data has also been declared as Protected System by National Critical Information Infrastructure Protection Centre.

National Informatics Centre (NIC), which provides IT/E-Governance related services to Government departments, protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place in the NICNET. NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems, anti-virus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardenings. These are complemented by round-the-clock monitoring of security events and remedial measures are carried out for solving the problems subsequently.

The Government websites host information for public dissemination and no sensitive information is hosted on such portals. As per the guidelines of the Government, the computer systems with sensitive information are isolated from the Internet. The content is managed by the respective Departments and the NIC officers are sensitized.

Additionally, NIC follows the advisories/instructions given by MeitY / other security agencies from time to time and issues guidelines, advisories, do's & don'ts etc. routinely for the benefits of its stakeholders with a view to secure the cyber assets, and these are published in the security portal for the internal consumption by its users.

*****