GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 6163
TO BE ANSWERED ON 04-04-2018

SEEDING OF BANK ACCOUNTS

6163. SHRI B. SENGUTTUVAN:

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

(a) whether the Constitution Bench of the Supreme Court of India hearing Aadhaar related cases has stayed indefinitely the Aadhaar-Seeding to bank accounts and mobile service operators and has permitted the linking only for the purpose of obtaining social benefits and if so, the details thereof;

(b) whether there is any constitutional mandate that the Government should be privy to all the personal details of one's life such as bank accounts, telephone usage, use of family rations etc. and if so, the details thereof;

(c) whether the disclosure of such information as the Aadhaar number, name of the person, his date of birth and communication address etc. would cause a serious threat to the security of individuals and if so, the details thereof and the corrective steps taken in this regard;

(d) whether there is a possibility that any person armed with the Aadhaar number, name and address of another person can thereby acquire the details of his bank account, access and operate the same and if so, the details thereof; and

(e) the safeguard put in place and measures taken to prevent the leakage of Aadhaar data?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K. J. ALPHONS)

(a): The Constitution Bench of the Supreme Court of India hearing Aadhaar related cases, has passed an interim order on 13th March, 2018, the relevant extract of which reads as under:-

"……on a query being made, Mr. K.K. Venugopal, learned Attorney General for India submitted that this court may think of extending the interim order. However, the benefits, subsidies and services covered under Section 7 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 should remain undisturbed.

Having heard learned counsel for the parties, we accept the submission made by the learned Attorney General. Subject to that, we direct that the interim order passed on 15.12.2017 shall stand extended till the matter is finally heard and the judgment is pronounced. That apart, the directions issued in the interim order shall apply as stated in paragraphs 11 to 13 in the said order. For the sake of clarity, we reproduce the said paragraphs which read as under:-

'11. In terms of (iii) above, subject to the submission of the details in regard to the filing of an application for an Aadhaar card and the furnishing of the application number to the account opening bank, we likewise extend the last date for the completion of the process of Aadhaar linking of new bank accounts to 31 March 2018.

12. In terms of (iv) above we extend the date for the completion of the E-KYC process in respect of mobile phone subscribers until 31 March 2018.

13. Consistent with the above directions, we also direct that the extension of the last date for Aadhaar linkage to 31 March 2018 shall apply, besides the schemes of the Ministries/Departments of the Union government to all state governments in similar terms. As a consequence of the extension of the deadline to 31 March 2018, it is ordered accordingly.'

It is also directed that the same shall also control and govern the Passports (1st Amendment) Rules, 2018."

(b): No, Sir.

(c): Under various provisions contained in the Sections 28 to 33 of Chapter VI of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, the UIDAI ensures the security, confidentiality of identity information and authentication records of individuals.

Besides, under various provisions contained in the Sections 34 to 43 of Chapter VII of the said Act, offences & penalties have been defined, inter-alia, for impersonations or attempts to impersonate another person with the intention of appropriating the identity of an Aadhaar number holder, changes or attempts to change any demographic information or biometric information of an Aadhaar number holder ; for disclosing identity information; for unauthorised access to Central Identities Data Repository (CIDR) ; for tampering with data in CIDR; for unauthorised use by requesting entity. Besides, the Aadhaar (Data Security) Regulations, 2016 also, inter-alia, provide for the measures for ensuring information security; security obligations of the personnel, security obligations of service providers etc.; confidentiality.

(d): No, Sir.

(e): 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. 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. Security is an integral part of the system from the initial design to the final stage. Security of Aadhaar data is monitored at all the times i.e. at rest, in transit and in storage. UIDAI has also been certified as per international standard, namely ISO 27001: 2013 by STQC in respect of Information Security Management System which has added another layer of IT security assurance. UIDAI-Central Identities Data Repository (CIDR) has been declared as a Protected System in pursuance of sub-section (1) of Section 70 of the Information Technology Act 2000 by National Critical Information Infrastructure Protection Centre.

Additionally, various policies and procedures have been defined clearly which are reviewed and updated continually; thereby appropriately controlling and monitoring any movement of people, material and data in and out of UIDAI premises, particularly the data centres. Physical security of UIDAI Data Centres is

being managed by armed CISF personnel. Further, strengthening of security of data is an ongoing process, and all possible steps are being taken in this regard. 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 thereunder have been specifically drafted keeping in account the various security requirements in respect of data collected by UIDAI.

******