GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4277
TO BE ANSWERED ON 18.03.2026

USE OF AADHAAR-BASED AUTHENTICATION SERVICE

4277. SHRI MANISH TEWARI:

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

(a) whether any Aadhaar data or Aadhaar-based authentication services are being used directly or indirectly in Artificial Intelligence (AI), Machine Learning (ML), predictive analytics or surveillance-related systems by any Government authority or agency;
(b) if so, the purpose, nature of analytics undertaken and the legal basis permitting such use;
(c) whether any agreements, memoranda of understanding or arrangements exist with third parties or other Government agencies enabling access to Aadhaar data or authentication services for AI-based or predictive analysis and if so, the details thereof;
(d) whether any audits or compliance assessments have been conducted to prevent misuse of Aadhaar data for surveillance purposes and if so, the findings thereof;
(e) whether any guidelines or Standard Operating Procedures govern data collection, retention, purpose limitation and privacy safeguards in such AI systems; and
(f) if so, whether these are likely to be placed in the public domain?

ANSWER

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

(a) to (f): Aadhaar is the world's largest biometric identity system maintained by Unique Identification Authority of India (UIDAI) with approximately 134 crore live Aadhaar holders. It has completed more than 17,000 crore authentication transactions.

Aadhaar authentication service of UIDAI:
UIDAI provides Aadhaar authentication service to authorized entities using which an individual's Aadhaar number and related identity information are verified with the Aadhaar database. This verification confirms the individual's identity using OTP, biometric (fingerprint, iris, face) or demographic details to deliver the services offered by such entity.

Aadhaar Face Authentication used by authorised entities is based on AI/Machine Learning technology which enables accurate authentication of face biometric.

Any entity desiring to use Aadhaar authentication services must be onboarded with UIDAI as Authentication User Agencies (AUA) or KYC User Agency (KUA), in accordance with the provisions of the Aadhaar Act.

Access to authentication logs:
Every AUA or KUA must retain authentication logs for two years. These logs can be accessed by Aadhaar number holder or can be shared for grievance redressal and dispute resolution. After two years, the logs are archived for five years and subsequently deleted.

Protection of Aadhaar data:
The Aadhaar ecosystem is designed to protect privacy, with demographic data remaining encrypted both at rest and in transit. The Aadhaar Act also imposes restrictions on the collection, retention, access, and use of Aadhaar data.

UIDAI has implemented a three-tier audit framework, comprising the Self-Compliance Audit, the Information Security Annual Audit, and the GRCP (Governance, Risk, Compliance, and Privacy) Audit, for entities in the Aadhaar Authentication Ecosystem.

This multi-layered approach ensures the integrity, security, and effectiveness of the ecosystem and helps mitigate risks to Aadhaar number holders.

The detailed Standard Operating Procedures (SOPs) and guidelines governing the collection, retention, access, and use of Aadhaar data are available in public domain. Key provisions include:

- Mandatory informed consent of Aadhaar Number holder
- Purpose-Agnostic authentication
- Aadhaar authentication only for predefined and explicitly permitted purposes
- Secure and limited authentication response
- Secure storage in Aadhaar Data Vault
- Use of certified devices only
- Limited and encrypted data retention
- No biometric data retention by any entity
- Mandatory audit trails

By design and architecture, the storage and processing of Aadhaar data takes place within India, and safeguards are in place to ensure that this is not breached.

****