GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1501
TO BE ANSWERED ON 12.12.2025

AADHAAR AUTHENTICATION AND SURVEILLANCE

1501. SMT. PRIYANKA CHATURVEDI:

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

(a) whether Aadhaar authentication or related data services are being integrated, directly or indirectly, with AI, ML, or automated analytics systems used by Central/State agencies or authorised third parties, if so, the details thereof;
(b) the nature of formal arrangements for Government or other entities to access Aadhaar data or authentication logs for analysis or decision support;
(c) whether audits, compliance checks, or independent evaluations have assessed risks of overreach, profiling, or surveillance from Aadhaar-linked datasets in automated systems, if so, the findings; and
(d) whether Government has issued SOPs, guidelines, or restrictions on collection, retention, access, or algorithmic use of Aadhaar data?

ANSWER

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

(a) to (d): Aadhaar is the world's largest biometric identity system maintained by Unique Identification Authority of India (UIDAI) with approximately 134 Cr live Aadhaar holders. It has completed more than 16,000 crore authentication transactions.

Aadhaar authentication service:
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 an AI/ML-based solution that enables smoother and more efficient delivery of benefits and services to individuals.

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 holders 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.

UIDAI has issued detailed Standard Operating Procedures (SOPs) and guidelines governing the collection, retention, access, and use of Aadhaar data. 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

****