Use of Aadhaar Biometric in Forensics

Why in news?

Recent discussions about using Aadhaar biometrics data to identify unknown dead bodies.

What are the challenges in finding identity with the current system?

- **Limited Records** - Fingerprint databases for police investigations are often limited to the records of those with known criminal histories.
- **Inadequate Digitization** - In many States, these records are not yet digitized, making it even more difficult to cross-reference data quickly and efficiently.
- **Under Reporting** – Many of the missing person cases are not registered with police, thus making it to difficult to identify the person.
- **Inadequate Evidences** - Victims of hit-and-run accidents without identification documents or mobile phones, or those with mental health issues and travelling to unfamiliar places.

What are the advantages of using Aadhaar in forensic?

- **Identification of deceased individuals –** Identification of unclaimed or unidentified bodies who are mostly migrant workers, homeless individuals.
- **Finding Missing Person –** Identifying missing or trafficked children, persons with mental health issues traffic.
- **Right to Life and Dignity –** Faster recognition of a deceased person enables for respectful final rites and closure for families.
- **Effective Crime Investigation** –Access to fingerprint data can offer essential scientific support to an investigation.
- **Enhancing Criminal Justice –** Effective investigation enhances the criminal justice system.
- **Uphold Public Safety** – Crime reduction using Adhaar improves public safety and reduces crime rate.

What are the limitations in using the Aadhaar in forensic?

- **Privacy Protection** - UIDAI takes privacy seriously, enforcing strict guidelines to protect individuals' demographic and biometric information.
- **Biometric Prohibition -** Section 33 of Aadhaar Act prohibits sharing of "core biometric information", which includes fingerprints and iris scans, with anyone for any reason.
- **Restriction in Access -** Section 33(1) of the Aadhaar Act allows the disclosure of certain information under an order of a court not inferior to that of a High Court judge.
- **Right to Privacy -** Supreme Court Judgement in Justice Puttaswamy case held Right

to Privacy as a fundamental right protected under Article 21.
- **Data Privacy Law -** Digital Personal Data Protection (DPDP) Act, 2023 protects the personal identity data of citizens.
- **Technical Limitation** - The technological architecture of UIDAI for Aadhaar-based authentication does not allow for matching prints , including latent and chance finger prints, against the other finger prints in the UIDAI database.

What lies ahead?

- Re-evaluating privacy restrictions in Aadhaar Act on specific contexts, such as identifying a deceased person.
- Providing the police with access to a deceased person's core biometric information, strictly based on a first information report (FIR).
- Enabling jurisdictional judicial magistrate to authorize the data access instead of High court judges to reduce the burden on the higher judiciary in cases not involving violations of privacy.
- Similar provisions might be adopted in India to ease identification challenges without compromising privacyImplementing legal and ethical guidelines with transparency can ensure Aadhaar's continued relevance and secure its place as a trustworthy public utility.

Quick Facts

- **UIDAI** – The Unique Identification Authority of India was established in 2009 to build a secure and centralized database that could help in the accurate identification of individuals across the nation.
- **Objective of UIDAI –** To streamline and secure identity verification processes, thereby reducing the risk of identity fraud and enabling individuals to access various governmental and non-governmental services.
- **Aadhaar –** It is a 12-digit unique identity number based on individual's demographic and biometric data, such as fingerprints and iris scans.

Reference

The Hindu |Aadhaar biometric data access will aid forensics