Misusing AADHAR data

What was the issue?

\n\n

Recently several disturbing incidents centred on the Aadhaar database have established the scope for widespread data leakage.

\n\n

What were the disturbing incidents?

\n\n

\n
- A technology start-up demonstrated that it could identify faces singled out from CCTV footage of a crowded street.
\n
- This firm is one of the many that offer services such as identity checks, PAN verification, police record checks and employment history generation by linking an individual’s data to his 12-digit Aadhaar number.
\n
- Another website filtered, compiled and published Aadhaar data to create a database listing of over 500,000 minors.
\n
- Several telecom salesmen selling Aadhaar data were arrested.
\n
- These events show the feasibility of parallel databases, which duplicate sensitive data.
\n

\n\n

How these parallel databases are built?

\n\n

\n
- The biometric identification system is being used extensively for e-KYC processes for multiple purposes.
\n
- At present, anybody can enrol as an agent to verify e-KYC.

\n
- But there is little to prevent such data being collected, stored and re-used for illegal purposes.
\n
- The application programming interface (API) for the Aadhaar e-KYC service is publicly available from the UIDAI.
\n
- Agent enrolment is a simple, quick process; the basic equipment is an inexpensive biometric fingerprint scanner connected to a smartphone.
\n
- KYC user agencies and service agencies access Aadhaar data after taking the individual's consent.
\n
- The individual must input a one-time password – delivered to a registered mobile number – to agree to authentication. The UIDAI only verifies queries with a binary "yes/no".
\n
- But the agency conducting the e-KYC and verification can collect and store data at its end.
\n

\n\n

What are the implications?

\n\n

\n
- Earlier white-hat hackers have demonstrated how iris scans can even be generated from high-resolution photographs.
\n
- Mobile service providers and banks have used private agencies to generate e-KYC data for hundreds of millions of people.
\n
- It is, therefore, possible that many parallel databases tied to Aadhaar already exist, and these Aadhaar numbers, in turn, are tied to other sensitive data.
\n
- The aggressive rollout also means that new databases continue to proliferate.
\n
- What makes matters worse is that there is **no specific privacy law or data-privacy law to stop such data being stored or traded**.
\n
- These security breaches suggest that any future privacy legislation, or

judgments by the judiciary, might only manage to close the door on data breach.
\n

\n\n

\n\n

Source: Business Standard

\n