Is Aadhaar a breach of privacy?

Background:

\n\n

Aadhaar was designed as a digital identity platform which is inclusive, unique and can be authenticated to participate in any digital transaction. Direct benefit transfer, subscription to various services and authentication at the point of service delivery are some of the benefits which have accrued.

\n\n

What are the in-built security features?

\n\n

- \n
- As UIDAI was creating identity infrastructure, it was decided that only a minimal set of data, just sufficient to establish identity, should be collected from residents.
- \n
- This irreducible set contained only four elements: name, gender, age and communication address of the resident.
- \n
- Another design principle was to issue random numbers with no intelligence.
- \n
- This ensures that no profiling can be done as the number does not disclose anything about the person.
- \n
- The Aadhaar Act has clear restrictions on data sharing.
- \n
- No data download is permitted, search is not allowed and the only response which UIDAI gives to an authentication request is ‘yes’ or ‘no’.
- \n
- No personal information is divulged.
- \n
- Aadhaar authentication and e-KYC ensures that documents cannot be misused.
- \n
- UIDAI has also built a facility wherein one can ‘lock’ the Aadhaar number and disable it from any type of authentication for a period of one’s choice,

guarding against any potential misuse.
\n

\n\n

What are the concerns?

\n\n

\n
- Biometrics allows for identification of citizens even when they don't want to be identified.
\n
- Even unconscious and dead citizens can be identified using biometrics.
\n
- Smart cards which require pins on the other hand require the citizens' conscious cooperation during the identification process.
\n
- If the UIDAI adopts smart cards, we can destroy the centralized database of biometrics just like the UK government did in 2010.
\n
- This would completely eliminate the risk of foreign government, criminals and terrorists using the breached biometric database to remotely, covertly and non-consensually identify Indians.
\n
- The Aadhaar Authentication Regulations 2016 specifies that transaction data will be archived for five years after the date of the transaction.
\n
- Even though the UIDAI claims that this is a zero knowledge database from the perspective of “reasons for authentication” - any big data expert will tell you that it is trivial to guess what is going on using the unique identifiers for the registered devices and time stamps that are used for authentication. .
\n
- Prohibit the use Aadhaar number in other databases.
\n

\n\n

What are the benefits?

\n\n

\n
- Aadhaar can plug these loopholes.
\n
- A Planning Commission study done six years ago on the Public Distribution System found 27 paise reaching the citizens.
\n

- The remaining 73 paise went on payments of salaries, administrative costs and corruption.
  \n
- District authorities are faced with large number of fake names or fake roll numbers, either for PDS or the mid-day meal scheme. That’s where Aadhaar can help.
  \n

\n\n

What is the way forward?

\n\n

  \n
- We need to educate people on the risks involved, and highlight examples of ID thefts and fraud.
  \n
- We have a multiplicity of laws which overlap.
  \n
- Our IT laws have to be modernised and we have to put the liability on the company handling the data so that it is not stolen or shared without consent.
  \n
- We need to take a level-headed approach and ensure that ample safeguards are put in place for data protection and privacy.
  \n

\n\n

\n\n

Source: The Hindu

\n