Privacy and Security in Aadhaar

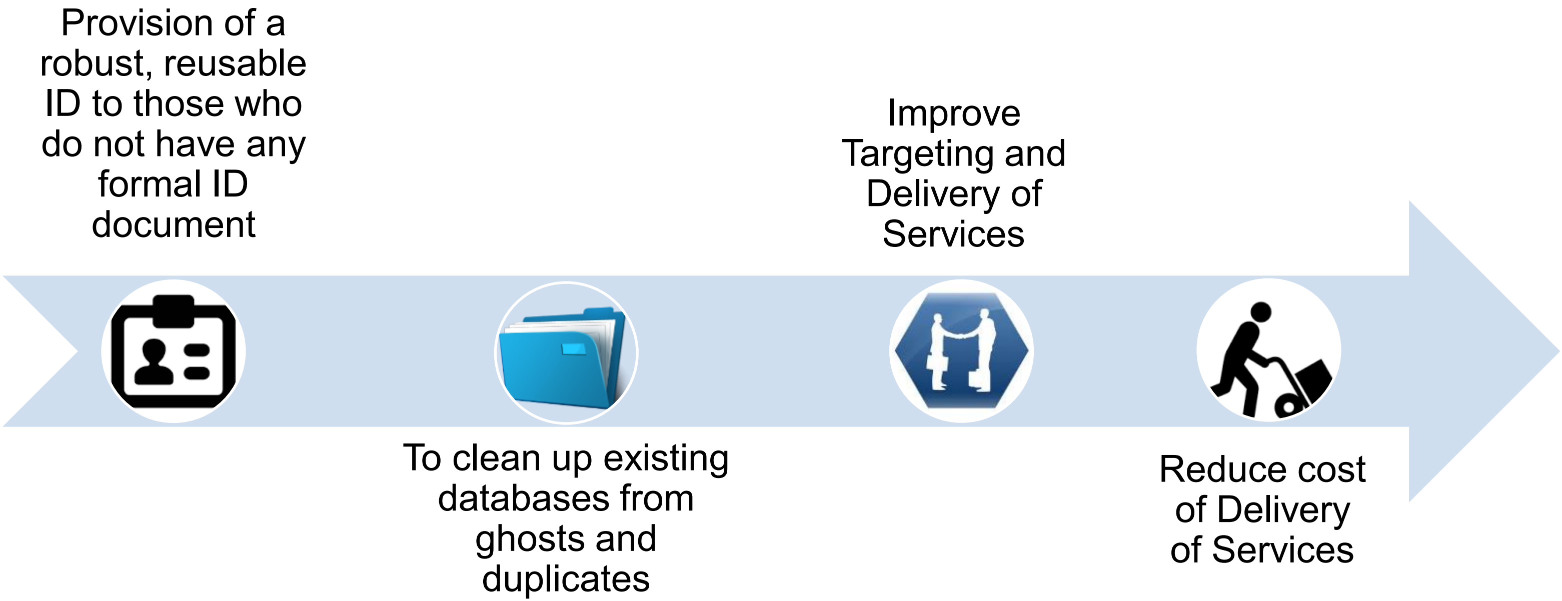
RS Sharma

rssharma3@gmail.com

Outline

- Context of Unique IDs in India
- Goals, features and Design Principles of Aadhaar
- Embedding Privacy in the design and operations
- Legal Challenges
- Technology Architecture of Aadhaar
- Conclusion

Context for a Unique Identity Infrastructure



Provision of a robust, reusable ID to those who do not have any formal ID document

To clean up existing databases from ghosts and duplicates

Improve Targeting and Delivery of Services

Reduce cost of Delivery of Services

Overarching goals

UNIQUENESS OF IDS

SCALE AND SPEED

EASE OF ACCESS AND PROCESS

INCLUSIVE AND SOLVES BOOT-STRAP PROBLEM

COST-EFFECTIVE

TECHNOLOGY TO UNDERGIRD

FUTURE PROOF

A PLATFORM AND NOT A PRODUCT

An Identity without Eligibility

- Just an ID: No rights or Entitlements
- Solves the Common Problem of many Domains
- Platform and Pluggable
- Authentication
- Foundational and not functional

Features of Aadhaar

- Only Numbers – No Smart Cards
- Random Numbers – No Intelligence, No Profiling
- Voluntary in nature
- All Residents – Including Children
- Uniqueness – Ensured through biometric attributes
- Just an ID: No Guarantees to Citizenship, Rights, Entitlements
- Ubiquitous Authentication – From No ID to Online ID

A few data points about Aadhaar

AADHAAR
Unique digital identity

Foundational, Designed for innovation
Secure and Privacy Preserving

1.36 Bn
IDs issued

860 M
ID linked bank accounts

470 Mn opened in last 8 years!!

150 Bn
ID authentications

1+ Bn auths / month

24 Bn
e-KYC transactions

Source: https://uidai.gov.in/

Principles of Privacy by Design

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default Setting
- Privacy Embedded into Design
- Full Functionality: Positive-Sum, not Zero-Sum
- End-to-End Security: Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy: Keep it User-Centric

Aadhaar Design Principles

- Minimal data collection
- Random number principle
- Biometrics
- No biometrics in Aadhaar ‘Card’
- No data sharing & no search
- Data always encrypted
- Federated Data Structure

Aadhaar Operating Principles

- Consent-based authentication: resident triggers authentication for service delivery.
- Notice about Authentication transaction
- End to end encryption during authentication
- Purpose Agnostic Authentication
- No linking Information - One way linking
- You may lock/unlock your biometrics

Legal Challenges faced by Aadhaar

- Challenged in Supreme Court through multiple PILs alleging violation of privacy and fundamental rights.
- This gave rise to two landmark decisions:
  - **Justice K.S. Puttaswamy (2017)** :Recognised **Privacy as a Fundamental Right** under Article 21.
  - **Puttaswamy (Aadhaar case, 2018)** : Examined Aadhaar’s constitutionality.
- Major Challenges
  - **Violation of Privacy** → State surveillance risk.
  - **Exclusion** → biometric failures could deny welfare.
  - **Proportionality** → less intrusive alternatives exist.
  - **Compulsory Linking** → with PAN, bank accounts, SIM cards.
  - **Money Bill route** → improper passage of Aadhaar Act.

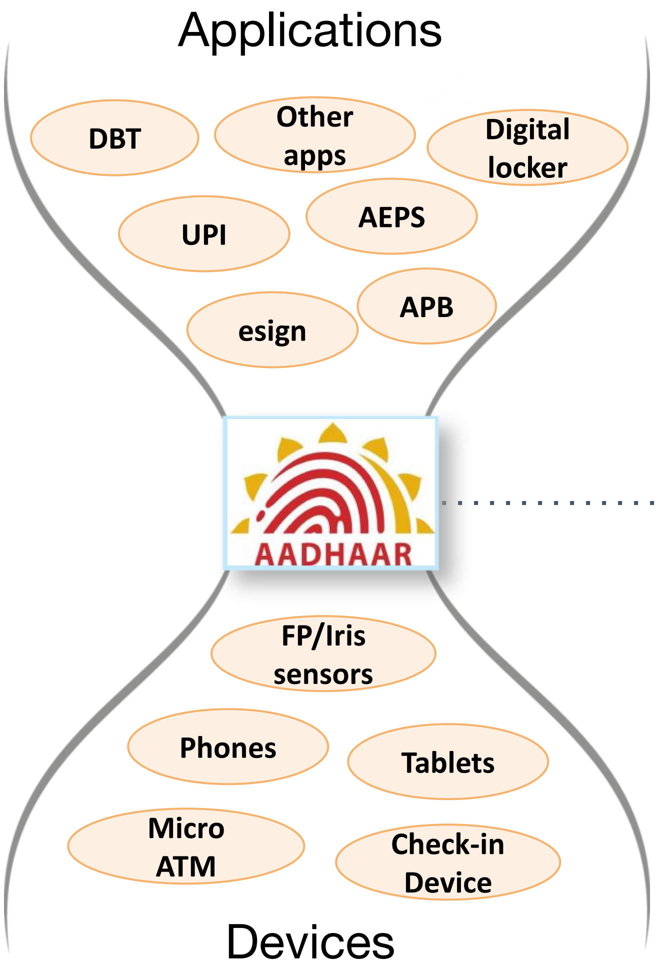
SC Judgement

Majority (4:1):

- Aadhaar is constitutional, passes proportionality test.
- Mandatory for subsidies/welfare & PAN–ITR linkage.
- Struck down for bank accounts, SIM cards, and private sector use.
- Directed stronger data protection measures.

Dissent (Justice Chandrachud):

- Entire Act unconstitutional.
- Money Bill route invalid.
- Surveillance & exclusion risks too high.



Applications

DBT

Other apps

Digital locker

UPI

AEPS

esign

APB

AADHAAR

FP/Iris sensors

Phones

Tablets

Micro ATM

Check-in Device

Devices

- Minimal
- Standardized

An 'hourglass' platform architecture

Allows innovation on all sides

Architecture Principles

- Understand the problem
- Break down into many services
- Build APIs to abstract logic & data
- Embrace open source
- Measure everything and believe in data
- Build failure resilience
- Scalability comes from the architecture
- Keep it simple and minimal!

Debunking the Fallacy *– Aadhaar Number contains no secrets that need to be guarded*

Nothing Secretive about a 12 Digit Number

Aadhaar number is less impersonal than the actual name of an individual or even phone number

No harm on Publishing Publicly

Even if published publicly, no harm can be caused to an individual using their Aadhaar Number alone. If any harm could be caused, providing Aadhaar at multiple places could have been dnagerous!

Zero Verifiable Security Breaches

Till date, no security breaches or such scandals have come to light or raised concerns on residents' privacy

Mathematical Proof by Manindra Agrawal, IIT Kanpur

'Analysis of Major Concerns about Aadhaar Privacy and Security'

- ❑ Analyzes differential privacy & security of Aadhaar Protocol
- ❑ Evaluates **3 kinds of attacks**: **Surveillance**, **Forgery** and **Database**
- ❑ Mathematical differential analysis on all three arguments **found non-negative**
- ❑ **Conclusion:** Disclosue of Aadhaar **doesn't increase digital vulnerability and privacy**; Need to ensure the security of key databases

There is no "reasonable expectation of Privacy" from Aadhaar. Hence, the actions taken to keep it hidden/encrypted/secret are absolutely meaningless – both legally as well as scientifically.

Data and Systems Security

Strong end to end encryption and audit

Data encrypted during enrolment

No decryption at any intermediate points

Every packet is biometrically signed by operator

Security best practices at CIDR

Data always encrypted “at rest”

Raw biometrics never stored unencrypted

Data and systems access audited and controlled

Data partitioned across multiple security “zones” separated by firewall and IPS

Key takeaways

Embed Privacy from the Start ("Privacy by Design")

Data Minimization & Purpose Limitation

Anonymization and Pseudonymization

User Control and Consent

Transparency and Accountability

Legal Guard rails (Aadhaar data not to be shared)

Key Takeaways

- Privacy-Preserving Technologies
- Data retention and right to forget
- Regular audits and monitoring
- Build for scale & diversity
- Legal and ethical Alignment
- Cultural mindset of respect
- Align with DPDP Act

Collect less, secure more, be transparent, give control, and always respect the individual.

Aadhaar is India’s first and the most transformational Digital Public Infrastructure (DPI). All subsequent DPIs draw from Aadhaar

Thank you