A Question of Identity: Overview

(Please see the main whitepaper for a full discussion.)

Soumen Chakrabarti* Siddhartha Chaudhuri* Om Damani*
Manoj Prabhakaran* Krithi Ramamritham* Bhaskaran Raman*
S Sudarshan*

Dept. of Computer Science and Engineering
IIT Bombay

A national identity scheme has long-term and large-scale implications to efficiency of governance, distribution of benefits, law enforcement and national security, welfare and data security of the people, and their privacy and other fundamental rights. Given the extensive criticism of the Aadhaar scheme, we propose that there should be an ab initio redesign of significant parts of the Aadhaar infrastructure.

We start with the following basic expectations on a national ID scheme:

- It must improve inclusiveness, empower the disenfranchised, and improve administration efficiency;
- It must help in curbing identity fraud;
- It must not lead towards disruption of access to essential services; and
- It must not lead towards violation of individuals’ fundamental rights.

Having reviewed several reports from the field, we conclude that the current Aadhaar design and implementation have extensive conflicts with the above expectations. For instance, a disturbingly large number of reports of denial of essential services, often due to reliance on biometrics for authentication in the field, have surfaced. While making certain forms of identity fraud harder, the widespread and loosely regulated use of the Aadhaar ecosystem (e.g., for authorizing financial and other transactions), has created room for several other forms of identity fraud. Also, privacy concerns, enhanced by the involvement of several private entities and weak data protection laws, have emerged. Some of these issues can be traced to fundamental design choices in the current Aadhaar implementation, like the use of biometric authentication, and the use of a centralized server accessed via “user agencies”.

Based on the lessons from this exercise, we formulate a set of technical design and policy guidelines for a national identity scheme that could avoid much of this conflict.

* Sorted alphabetically. Email: {soumen,sidch,damani,mp,krithi,br,sudarsha}@cse.iitb.ac.in
Guidelines

We present a non-exhaustive list of guidelines which we believe are important for a national identity scheme.

- **Avoid confusion/conflation of identification, authentication, and authorization.** The current Aadhaar ecosystem is being used for unique identification, for authentication, for “Knowing Your Customer” (KYC), for authorization, as a convenient repository for multiple certificates/documents, etc. But Aadhaar’s design does not directly support all these uses: For instance, many applications (e.g., property registrations in Maharashtra) offer ad hoc protocols to carry out authorization based on Aadhaar’s biometric authentication, and in the process creates room for fraud. Such conflation of different goals and the means to achieve them makes the system exceedingly complex and vulnerable to unforeseen exploitation. Our first guideline is therefore to separate out these different purposes, and specify them formally. UIDAI must give precise guidelines as to what purposes Aadhaar can and cannot be used for.

- **Minimize dependence on biometrics.** While sufficiently detailed biometrics can be effective in deduplication (unique identification), they are a poor choice for authentication, as they are irrevocable and easy to steal. Collecting biometrics of citizens also raises privacy concerns, and has led to resistance in countries like Israel and UK leading to reversal of policies. Aadhaar usage statistics so far reveals a significant rate of biometric errors when deployed at a massive scale. Hence, the use of biometrics, if any, should be only as an aid to deduplication at the time of enrolment. Biometrics should be collected or verified at high security levels (e.g., comparable to that in passport offices), and never by third parties who may be easily compromised.

- **Minimize the need for live network interaction** with remote servers, to avoid disruption of essential services, to mitigate the effect of potential cyber attacks, and to reduce the collection of tracking data.

- **Maximize privacy guarantees** via technological and policy design. For instance, the identification functionality can reduce or even remove the need for service providers to collect KYC information, and also prevent them from tracking a user across multiple services. Yet, there can be technological provisions (protected by a strong legal framework to prevent abuse) for tracking individuals when there is due cause, with the active participation of multiple stakeholders and watchdogs.

- **Maximize availability guarantees**, with respect to both overall system availability and each individual’s access to services. In particular users should be protected against a “kill switch” in the same way they are protected against tracking.
• **Assume some users, service providers and insiders will be compromised** and may collude with each other. Even so, the system should retain the above security and availability guarantees. Towards this, a defense-in-depth approach should be used, possibly combining cryptographic techniques and open-specification secure hardware.

• **Allow individuals control over enrolment and usage.** Enrolment should be truly voluntary and there should be a mechanism for users to remove themselves from the system (possibly with safeguards for tracing fraudulent activities). Any services built on the identity scheme should be required to provide reasonable alternatives for those who have not opted in or choose not to use the system at any point of time. There should be wide-spread awareness about the restrictions on third party service providers.

• **Plan for exceptions and evolving design.** Exceptions are inevitable in a nation-scale system. There should be responsive and humane protocols in place to handle exceptions for individual users without unduly inconveniencing them, and if necessary temporary workarounds should be facilitated. There should also be a provision for protecting users against any damages caused by errors and exceptions in the system. The system design will evolve over time and there should be plans to update the deployment in a phased manner.

• **Independent monitoring.** To ensure efficiency, security and fairness of the implementation, an independent agency should regularly monitor various aspects of the system regularly including grievance redressal, compensation for damages, and conduct security audits.

These guidelines provide us with a means to evaluating current and future proposals for Aadhaar. As the current design is seen to have serious shortcomings with respect to these guidelines, we recommend that it be considered experimental and used accordingly. Any parts of the existing system retained in a subsequent design (for minimizing implementation costs) should not be at the expense of the above design goals. Designing and deploying a robust identity scheme for the largest democracy in the world will require much more thought, wider expert consultation, and a few more years.