Do we need the Aadhar scheme?

Its guarantee of non-duplication can have far-reaching cost benefits but it has deep design flaws that can be compromised.

PRAVEEN CHAKRAVARTY

Former Volunteer, Financial Inclusion, UIDAI (*Currently CEO of an investment bank*)

"Aadhaar is an unadulterated identity programme that answers the question: Is the individual who he or she claims to be?"

The word "unique", and not "identity", is central to the unique identity programme or Aadhaar.

It may be true that the vast majority of people possess some proof of identity — voter ID, ration card, PAN card and so on. But most of it is not unique, that is to say, there is a proliferation of duplicate or false identities. Many state governments have acknowledged this problem and independently embarked on various initiatives to "de-duplicate". These include the iris-based public distribution system (PDS) cards in Andhra Pradesh, hologramised cards in Gujarat, "smart" cards in Tamil Nadu and so on. With an Aadhaar, there is an absolute guarantee that no two people will have the same Aadhaar, and it cannot be duplicated either. This is a powerful proposition to plug leakages in the delivery of Rs 3 lakh crore ($60 billion) worth of government welfare subsidies every year.

Aadhaar's use of the "natural" identity of humans such as biometrics and iris scans ensures that it is non-duplicable. The cost benefits of the project can be immense and immediate. The Unique Identification Authority of India's (UIDAI's) clever use of an outsourced enrolment-model limits its direct cost to only Rs 50 a person for enrolment and the total estimated project cost to Rs 6,000 crore for enrolling 600 million people. To put this in context, the food subsidy outlay alone in last year's Budget was Rs 60,000 crore and most state governments estimate that, on average, five per cent to 12 per cent of ration cards are duplicate. A simple calculation assuming a five per cent duplicate rate of subsidised foodgrain consumption implies a potential saving of Rs 3,000 crore in our PDS alone.

Aadhaar is an unadulterated identity programme that answers the question: Is the individual who he or she claims to be? However, it cannot establish if that individual is poor or rich, legal or illegal, an Indian citizen or a foreigner, a terrorist or an angel and so on. There seems to be a lurking fear that Aadhaar can legalise the illegal, make the ineligible eligible. This fear is unfounded because the mere possession of an Aadhaar does not entitle any rights nor does it provide any eligibility information for such rights. For example, the home ministry may be interested in citizenship status, the food and civil supplies ministry in PDS eligibility status or the Election Commission in the eligibility to vote. Each of these bodies define their own criteria for such eligibility and then map the individual’s Aadhaar number, thereby creating a database of eligible Aadhaars instead of having to issue their own ration or voter or National Rural Employment Guarantee Act (NREGA) card.

It is the great irony of democracy that people believe the government they elect is innately malevolent. Hence the concern that the State can use the Aadhaar database for racial profiling, individual targeting and so on. This is unwarranted because the only information that Aadhaar collects for its database is an individual’s name, address and date of birth. Other concerns about privacy rights are equally misplaced. In today’s social media age – in which millions of people volunteer vast amounts of personal information – to argue that a government programme that collects basic demographic information is a violation of privacy rights, is plain egregious.

There have been some misgivings about the technological risk involved in the project, that is, can fingerprints be a reliable identity parameter given the vast number of farm workers in our country that are engaged in hard manual labour? UIDAI is confident that a combination of 10 fingerprints and two iris scans per person is enough to prove identity among a population of 1.2 billion. At 170 million enrolments currently, it is already the world’s largest biometric database with no signs of any technology risk.

Most of the debate on Aadhaar stems from the lack of an immediate application for Aadhaar that can demonstrate cost benefits, service delivery improvements and lack of technology risk and is instead viewed as some esoteric “identity platform”. There is some legitimacy to these concerns and these could have been avoided had Aadhaar been launched with a programme like PDS or NREGA to showcase how this would work.

The Indian Express, on January 27, reported how the same person was awarded with the Padma Shri twice through a mere change in the spellings of his surname and domicile. Clearly, there are more uses for Aadhaar than just welfare services delivery!

Do we need the Aadhar scheme?

Sunil Abraham

"Decentralisation and privacy are preconditions for security. Digital signatures don’t require centralised storage and are much more resilient in terms of security", Sunil Abraham in the Business Standard on 1 February 2012.

We don’t need Aadhar because we already have a much more robust identity management and authentication system based on digital signatures that has a proven track record of working at a “billions-of-users” scale on the internet with reasonable security. The Unique Identification (UID) project based on the so-called “infallibility of biometrics” is deeply flawed in design. These design disasters waiting to happen cannot be permanently thwarted by band-aid policies.

Biometrics are poor authentication factors because once they are compromised they cannot be re-secured unlike digital signatures. Additionally, an individual’s biometrics can be harvested remotely without his or her conscious cooperation. The iris can be captured remotely without a person’s knowledge using a high-res digital camera.

Biometrics are poor identification factors in a country where the registrars have commercial motivation to create ghost identities. For example, bank managers trying to achieve targets for deposits by opening benami accounts. Biometrics for these ghost identities can be imported from other countries or generated endlessly using image processing software. The de-duplication engine at the Unique Identification Authority of India (UIDAI) will be fooled into thinking that these are unique residents.

An authentication system does not require a centralised database of authentication factors and transaction details. This is like arguing that the global system of e-commerce needs a centralised database of passwords and logs or, to use an example from the real world, to secure New Delhi, all citizens must deposit duplicate keys to their private property with the police.

Decentralisation and privacy are preconditions for security. The “end-to-end principle” used to design internet security is also in compliance with Gandhian principles of Panchayat Raj. Digital signatures don’t require centralised storage of private keys and are, therefore, much more resilient in terms of security.

Biometrics as authentication factors require the government to store biometrics of all citizens but citizens are not allowed to store biometrics of politicians and bureaucrats. The state authenticates the citizen but the citizen cannot conversely authenticate the state. Digital signatures as an authentication factor, on the other hand, does not require this asymmetry since citizens can store public keys of state actors and authenticate them. The equitable power relationship thus established allows both parties to store a legally non-repudiable audit trail for critical transactions like delivery of welfare services. Biometrics exacerbates the exiting power asymmetry between citizens and state unlike digital signatures, which is peer authentication technology.

Privacy protections should be inversely proportional to power. The transparency demanded of politicians, bureaucrats and large corporations cannot be made mandatory for ordinary citizens. Surveillance must be directed at big-ticket corruption, at the top of the pyramid and not retail fraud at the bottom. Even for retail fraud, the power asymmetry will result in corruption innovating to circumvent technical safeguards. Government officials should be required by law to digitally sign the movement of resources each step of the way till it reaches a citizen. Open data initiatives should make such records available for public scrutiny. With support from civil society and the media, citizens will themselves address retail fraud. To solve corruption, the state should become more transparent to the citizen and not vice versa.

UIDAI’s latest 23-page biometrics report is supposed to dispel the home ministry’s security anxieties. It says “biometric data is collected by software provided by the UIDAI, which immediately encrypts and applies a digital signature.” Surely, what works for UIDAI, that is digital signatures, should work for citizens too. The report does not cover even the most basic attack — for example, the registrar could pretend that UIDAI software is faulty and harvest biometrics again using a parallel set-up. If biometrics are infallible, as the report proclaims, then sections in the draft UID Bill that criminalise attempts to defraud the system should be deleted.

The compromise between UIDAI and the home ministry appears to be a turf battle for states where security concerns trump developmental aspirations. This compromise does nothing to address the issues raised by the Parliamentary Standing Committee on Finance, headed by the Bharatiya Janata Party’s Yashwant Sinha.