A judgment without aadhaar

Subhashis Banerjee

Computer Science and Engineering, IIT Delhi
New Delhi 110016

December 7, 2018

The Aadhaar case has raised some serious and complex questions, but the arguments in the Supreme Court and the judgments did not engender confidence in the process, particularly in the court's ability to deal with issues of technological nature.

Aadhaar always had a theory of exclusion due to uncertainties in biometric matching which was largely ignored by the government and the bureaucracy, but its theories of inclusion and efficiency were never adequately developed. Clearly, a lot more than Aadhaar need to be in place to empower citizens to receive their entitlements. This crucial gap in Aadhaar, compounded with the brazen overreach in some situations without explanation or rationale, resulted in misgivings among people and set an example of how not to do technological innovations in public policy.

However, lack of credible theories of inclusion and efficiency does not imply that such theories are not possible, and one had hoped that some wisdom may emerge through the court proceedings. But the rhetorics and hyperboles, and the superficial understanding of technological aspects manifested in not only the arguments but also in the judgments - both in the majority and in Justice D Y Chandrachud's (DYC) dissent - have left one disappointed. Aadhaar continues with its theory of exclusion unmodified, but the possible theories of public good are as incomplete as ever.

This raises serious doubts about the courts ability to deal with technological questions. The court may not be the best place to resolve differences on technology based public policy interventions. In any case, Aadhaar is unlikely to be the last one such, and the court needs to develop better methods.

The majority's endorsement of Aadhaar as a money bill can only be a reflection of their helpless acceptance of the fait accompli. However, that the government has resorted to dubious stratagem does not establish that the instrument is unsound. The other challenges before the court were based on arbitrariness, exclusion, violation of dignity, privacy and liberty, surveillance, overreach, excessive delegation and retrospective validation of infringement of rights; and the court had to decide whether or not Aadhaar was beyond redemption.

The majority and DYC agreed that there is a legitimate state aim in ensuring uniqueness and targeting for welfare. They also broadly agreed on the three-pronged proportionality test for the constitutionality of Aadhaar based on determination of rational nexus between the objectives and the means, of necessity - implying that the adopted means are the least intrusive for the purpose - and of balancing of extents to which rights are infringed. They however were disconcertingly contradictory in their determination of outcomes, mainly due to their disparate interpretation of technological issues. Their tests were based on the following main concerns.

First, while the majority accepted that biometrics ensured uniqueness and disregarded the implications of false positives in matching, DYC found the probabilistic steps in de-duplication unacceptable. Both positions are extreme. Randomized algorithms are ubiquitous, and protocols cannot be discarded merely because they are probabilistic. For example, even establishing secure internet

connections require crucial probabilistic steps, and all digital electronic components are designed using probabilistic analysis. One needs to avoid the rhetoric and obtain precise quantitative bounds to determine the efficacy of de-duplication. A study in the petitioners' submissions theoretically projected the false positive rate to be about 1%, which would mean that almost everybody would falsely match with another making enrolment of 1.2 billion impossible. However, estimated projections need validation by controlled experiments with random selections of people. Such an audit would have also put to rest all speculations about the uncertainties of the enrolment process. It is amazing that neither did UIDAI provide such data nor did the court ask for it.

De-duplication can tolerate some false positives because gaming it would require finding somebody's biometric Aadhaar-twin, which, even among a hundred people, has no easy solutions. However, exclusions due to false negatives during authentication are unacceptable because the welfare entitlements derived from NFSA and NREGA are unconditional. In view of this, the majority's decision to uphold biometric authentication and not read down Aadhaar is baffling. Striking down online biometric authentication would also have removed much of DYC's concerns regarding identity theft, impersonation risks and privacy violation due to biometrics.

Second, to decide on whether biometrics are the least intrusive for the state aims of de-duplication and identity verification, the majority put the onus of proof on the petitioners, and DYC on the respondents. However, in the absence of any credible analyses and design alternatives, there can be no basis for any such claims, either way. The petitioners had vaguely suggested smart cards for authentication without any supporting process design, or even articulating the design objectives. It begs the question that if Aadhaar has persistent linking errors, then how can similar administrative practices make a smart card linking process error free? And, nobody has even mentioned any alternative to biometrics for de-duplication, though that does not imply that there can be no such.

Third, balancing of rights required determining the exact nature of infringements on privacy and dignity. The privacy challenge was based on possibilities of surveillance and profiling through linking of databases and through Aadhaar meta-data. However, the analyses from both sides were exaggerated.

For example, suppose that the Aadhaar linking information were taken out of these various databases. Would profiling through linking still be possible? Almost certainly, using demographic details, phone numbers etc., even without using many sophisticated data mining techniques. So, Aadhaar does not differentially add to the linking risks significantly, which DYC failed to acknowledge. The key to privacy protection then is access control to these databases for which even the Srikrishna committee's draft data protection bill fails to provide any guidelines, and the majority simply assumed that access control is foolproof.

The State Resident Data Hub (SRDH) initiatives of several states were neither well thought out nor backed by any law. They were clear cases of overreach of Aadhaar that needed to be struck down. But it does not logically follow from these poor applications that Aadhaar itself is unconstitutional.

The petitioners claimed that Aadhaar meta-data enabled surveillance by determination of purpose and location of transactions, despite the respondent's assurance that they do not store or infer purpose or locations. In contrast, the respondents asserted that Aadhaar logs are 'zero-knowledge' and dared the petitioners to glean information out of the UIDAI chief's authentication logs. Both are hyperboles. DYC concluded that locations are easily determined from meta-data and IP addresses, without providing any theoretical basis for the claim. An affidavit submitted by Manindra Agrawal from IIT Kanpur did address some of these issues, but its selective and narrow interpretation by DYC was surprising. The majority too found that the logs violated the principles of data protection.

Determination of location from such meta-data, especially from historical data, unless explicitly recorded, will be uncertain even with complete access to the requesting entity's or network ser-

vice providers' meta-data. Logs and meta-data are essential parts of any digitisation, and privacy protection requires strict access control regulations. The majority's dictum that meta-data should be deleted after six months serves no real purpose and actually hampers audit and diagnostics. It is undeniable that indiscriminate access to UIDAI's logs poses privacy risks, but the telecom service providers' perhaps even more so. The solution lies in a strong regulatory framework for data protection which needs to go much beyond Aadhaar.

Also, licensing software from vendors without source code is routine, and that does not usually imply that vendors can have free access to operational data or can transfer them out. This can be no reason for calling an instrument unconstitutional.

'Bodily violations' and 'indignity of biometrics' were another set of dubious arguments. Biometrics are not innards; they are mere images of exposed body parts similar to facial photographs, which have commonly been used for identity verification for ages. And, just because it is common to fingerprint criminals, it is flawed to abductively conclude that fingerprinting implies a presumption of criminality. Moreover, the right of choice surely needs to be balanced with administrative imperatives? There may be anarchy if we insist on obtaining ration or being identified for taxes using any card of our choice. Besides, it appears infructuous to conflate digital identities for conducting businesses with our constitutional right to multiple social and cultural identities. Surely, some rigorous sociological studies are required.

Amidst all the din and the over-emphasis on privacy, some of the most objectionable aspects of Aadhaar were not adequately examined. Apart from exclusion, perhaps the most dire is the non-federal, non-social definition of digital identity by an opaque, centralised bureaucracy. This is distinct from centralised storage which is at best an engineering issue.

Technology has no agency, and the 'vicissitudes of technology' arise mainly because of the poor selections and applications that result out of lack of rigorous analysis. Even after the Aadhaar judgment, the understanding required for judicious design of a de-duplicated, self-sovereign digital identity that has a theory of common good and is respectful of rights and conveniences of people remains as elusive as ever.