An argument without Aadhaar

In the Aadhaar debate, which has panned out mainly through op-ed articles and TV shows, strident dogmatic positions have far outnumbered credible peer reviewed analyses, and the proponents and opponents have mostly talked past each other. Detailed reports from institutions engaged in policy studies have been far and few. The government and the UIDAI have decided to brazen it out and have not engaged enough with civil society activists and researchers. These have resulted in overall confusion and mistrust.

There have been alarming reports of exclusion and disruption in social welfare but it is still unclear whether they are due to fixable teething troubles, careless deployment or something more fundamental, and what proportion is affected. Besides, neither have the opponents been able to make precise how exactly does Aadhaar violate privacy, nor have the UIDAI and ministerial proclamations declaring Aadhaar to be perfectly safe engendered confidence. Moreover, trivial and easily fixable examples of privacy breaches have been turned into big issues.

Whatever were the initial plans, the government clearly wants to use the unique identification of Aadhaar to enforce compliance in a variety of schemes by avoiding duplicates. The opponents want that Aadhaar must be voluntary - and so be it if that makes it a lame duck instrument. And, the potential benefits of Aadhaar beyond de-duplication, for example in analytics, have not even been discussed much!

The disagreement has inevitably shifted to the court. However, in the recent Aadhaar-PAN linkage case, several arguments from both sides were specious and not well analysed. No expert was examined and the judgment - though perhaps fair under the circumstances - did not inspire confidence in the process. The court is perhaps not the best place to decide on suitability of social policy interventions.

For example, the petitioner's argument on *legislative competence*, that the linkage cannot be made mandatory in the IT Act without first removing the contradiction from the original Aadhaar Act, appeared to be compelling. Yet the court dismissed it, though it was perhaps touch-and-go. However, even if the court had upheld it, the objection was more on procedural grounds and not fundamental in nature, and at best the government would have been forced to go back and amend the original act.

The petitioner's arguments under Article 14, that the mandate discriminates between different classes of tax payers, must have sounded tenuous even to the petitioners and were summarily rejected. The arguments under 19(1)(g) that PAN cancellation violates the right to practice any profession were accepted, but so were the state's arguments on need for de-duplication. The court also accepted, without question or calling for any analysis, the state's assertion that biometric de-duplication is perfect! Partial relief was given to non-Aadhaar holders on the ground that cancellation of PAN will cause hardship.

The petitioners had put forth another set of problematic arguments based on dignity and bodily autonomy, on the state's right of eminent domain over the human body and on informational self-determination. The court deferred them for consideration by a larger bench, along with all issues related to privacy. The mandated use of Aadhaar for IT is egalitarian, and any perceived indignity of fingerprinting is due to prejudice. Moreover, fingerprints and iris scans (both can be contactless) are fundamentally not different from facial photographs; they are images and not parts of one's body. They can all be used for matching and de-duplication either manually or automatically. They differ only in efficacy and not in principle, and one is not a bodily violation if the others are not. Unfortunately, the response from the state - claiming that the state indeed has a right over the human

body - was irrelevant and even more disproportionate!

The question then is - can the state insist on an identification mechanism? If so, under what circumstances? What are the limits of informational self-determination? Note that the state has already assumed this right, many years back without much protest, by making PAN cards with photographs mandatory for tax returns. The sole purpose even then was de-duplication, only the methods and efficacy were different.

So, the main issue is privacy, which the court has been deferring, and little has been said on it to enable an informed decision. On the one hand, the state's position that Aadhaar is safe because UIDAI stores only minimal data required for biometric matching and demographic details, is untenable. The government and UIDAI cannot absolve themselves of the responsibility of protecting users from privacy breaches through possible correlation attacks on linked databases. Further, the possibilities of insider attacks also need to be considered.

On the other hand, the opponent's claim - that collecting biometric information and storing them in a central database, and linking multiple databases through the Aadhaar number, fundamentally violates privacy and opens door for mass surveillance - is also without any careful evaluation of a precise threat model. For example, PAN cards are already linked to bank accounts, ITR and major purchases - how does linking Aadhaar increase the possibilities for correlation attacks? Why is making the Aadhaar number public more dangerous than making PAN public? If someone publishes her ten-prints, iris scans and Aadhaar number along with demographic details in a newspaper, how exactly her privacy may be compromised? Biometric and demographic details are publicly available anyway, and anybody determined enough can obtain these from touched objects and using a powerful camera even without the victim's cooperation. Clearly, it will be unsafe and preposterous to use biometrics for authentication, for example to access bank accounts, but what about only for identity verification and de-duplication? Surely we need to exhaustively enumerate the possible ways in which privacy may be compromised and model an attack surface? Only then can the questions related to privacy protection, either through technical or legal means, even be asked. The oft repeated assertion that privacy protection is impossible with biometrics and a global id is far from established.

It may not be enough to apply traditional understanding of privacy to the new scenarios presented by digital identity and the internet. The need of the hour is for our institutions to wake up and carry out conservative, detailed and rigorous analysis of all issues involved - social, economic, technical and legal. Till then, it will be best to go slow with Aadhaar, engage, analyse, correct, and ensure that there are no hardships.