Aadhaar Bill Debate: Raju Rajagopal

Q: The government already has the means to collect a lot of information on citizens (example, phone conversations and logs, credit card transactions, income tax records, bank account details, etc.). Conversely, there are many activities which happen under the radar (example, cash transactions, informal sector employment, etc.). What kind of information gathering powers will Aadhaar confer on the State over and above what it already has? Can you give specific examples of incremental power?

Demographic information in the *Aadhaar* database is so limited (name, gender, birth date, and address) when compared to other sensitive personal information mentioned above, and the restrictions against divulging both demographic and biometric information even to other arms of the government are so stringent, that I do not see *Aadhaar* in itself conferring any new information-gathering powers on the State.

Aadhaar is mandated only for government subsidies, as per the *Aadhaar* Law, and the only incremental power it gives the State is better ability to rein in massive leakages of public funds, as already demonstrated in the case of LPG (liquefied petroleum gas). The Supreme Court is likely to remain the final arbiter of which programmes may require *Aadhaar* and, as in the past, it is sure to call out any overreach by the government.

Had *Aadhaar* been mandated for other services such as telephones, bank accounts, etc., it would certainly have conferred considerably more power on the State as well as on private players. So, it is reassuring to see that the government is letting *Aadhaar* holders themselves decide where they would like to draw the line between convenience and privacy. In this context, it is worth noting that UIDAI (Unique Identification Authority of India) offers a “Biometric Locking” feature, which allows a resident to effectively opt out of *Aadhaar*, should she/he be concerned about data privacy.

If I have one wish about the incremental power that *Aadhaar* could give to the government, it would be the ability to mandate *Aadhaar* authentication for all property registrations, which are steeped in irregularities.

Q: The Supreme Court verdict that Aadhaar cannot be made mandatory to receive benefits reflects the concern that it may increase exclusion errors, either by leaving people out of the net or through technological malfunction. Is this a serious concern?

A legitimate concern in the early days of UIDAI (Unique Identification Authority of India) was that it too might exclude millions of Indians who have no acceptable proof of ID. That was the genesis of the “Introducer” concept, which allows such residents to enroll based on affidavits by certain designated “well-known” persons. Unfortunately, local Registrars responsible for appointing Introducers have had no incentive to actualise the concept and consequently very few people have been enrolled using this exception route.

Yet, looking at statistics presented by the government (example, 93% of adults enrolled to date) it seems that UIDAI has found other ways to enroll such vulnerable groups. It will likely make more special efforts to do so in the coming months, as now required by the *Aadhaar* Law. There is already talk of special enrolment camps and mobile enrolment vans to reach out to remote/infirm populations.

Given the above, I have a lot more confidence today that *Aadhaar* will indeed cover the last mile to reach previously excluded groups. Looking back, however, had NGOs that work with under-served communities taken a more proactive role in the enrolment process, faster progress could have been made on this front. Sadly, many prominent NGO leaders have taken an adversarial view of *Aadhaar*, and UIDAI on its part has been reluctant to welcome NGOs as true partners.

In the meantime, it is worth noting that the *Aadhaar* Law requires that no one otherwise eligible for government subsidies may be turned back just because they do not have *Aadhaar*. UIDAI has recently made reference to this provision as well as to potential exclusions due to technology failures and has stated that the upcoming *Aadhaar* Regulations will make adequate provisions to mitigate exclusion errors.

Q: On the other hand, supporters express the hope that Aadhaar will reduce inclusion errors and corruption by eliminating ghost beneficiaries, say in schemes like MNREGA (Mahatma Gandhi National Rural Employment Guarantee Act). Are there substantial benefits to be reaped on this account?

There is no question that the use of *Aadhaar* to de-duplicate databases can be very effective in eliminating ghost and duplicate beneficiaries. The example of LPG, where the government claims to have saved over Rs. 150 billion in the “initial stages alone”, only reinforces the anecdotal evidence that *Aadhaar* and the Direct Benefit Transfer (DBT) Scheme linked to it, are beginning to have a significant positive impact on the ground.

It is unfortunate that some critics are set on trivialising the issue of “wrongful inclusions” in public subsidy programmes and question the demonstrable savings in LPG subsidies by arguing that some of those savings could have been achieved even without *Aadhaar*. They ignore the fact that numerous attempts by states to de-duplicate beneficiary databases using electricity meter numbers, ration card numbers, etc. have previously failed; and such efforts were one-time or episodic at best, while *Aadhaar*-based de-duplication is a continuous and sustainable process over time.

Yes, there are theoretically other alternative tools to *Aadhaar* to help weed out ghosts and duplicate beneficiaries, but such tools have often themselves been suspect and have led to questionable results. That is the true import of a credible lifetime ID such as *Aadhaar*, whose efficacy as a “Unique ID” has not been seriously challenged so far, which can be used not only for de-duplication but also for real-time authentication of beneficiaries.

In my view, technology has often been more effective as a change agent in India than all the moralising and threats of punitive actions (example, ra tax returns, etc.). And *Aadhaar* has the true potential to become the backbone of such a technology-lead anti-corruption effort at the point of service delivery.

Q: Most advanced economies have had some version of UID for a long time, example, the Social Security number in the US, the Social Insurance Number in Canada, etc. This is recorded not only in interactions with the State (example, tax filing) but also in many kinds of non-governmental transactions (example, college admissions or property purchase). Yet, it is arguable that these nations have not become police States, occasional abuse notwithstanding. If privacy concerns in India are justified, is it a reflection of the trust deficit in government specific to India (or poorer countries more generally)? Or do you think schemes like UID inevitably lead to a surveillance State anywhere in the world?

I do not think that the trust deficit in government is specific to India or to poorer countries: example, poll after poll in the US show very high levels of mistrust in their government. The difference between the two countries, however, may be that Americans tend to trust their personal information with private agencies more than with the government (despite the fact that the largest data breaches have come from that sector!) while Indians have historically entrusted their personal information more to the government than to private agencies (which is changing rapidly with the proliferation of online transactions). In any case, it is ironic that activists who are at the forefront of the fight for a larger government role in poverty alleviation in India are also often the most distrustful of the government when it comes to data privacy.

Depending upon one's definition of a surveillance State, one could make a case that both the US and India are already there, especially in the context of their 'fight against terrorism' and the virulent strain of 'nationalism' currently infecting the Indian polity. The real question is whether fears of large-scale misuse of personal data by the government are justified.

In my view, if such fears were real, India would have already be an Orwellian State, given the ubiquity of personal data generated by mobile phones and the internet in recent years. Thankfully, that has not happened; and there is no credible reason to believe that adding *Aadhaar* numbers to the mix is going to dramatically change the situation. Having said that, it is still incumbent upon the government to do all it can to ease the concern over potential misuse of data. For instance, it could commit to periodic reporting of the *number* of exceptions made to data access under clause 33 (that is, via order of the courts and/or for national security).

Q: Can something like UID be created without compromising privacy beyond acceptable limits? If so, how should the Aadhaar Bill have been written? What are its specific and avoidable weaknesses?

Early critics of *Aadhaar* had argued that a comprehensive data privacy law must be enacted *before Aadhaar* came into existence. I strongly differed from that view, as any realistic effort to define boundaries of data privacy can only grow out of people's actual experiences in our fast-changing tech-world. If the rush by the urban middle class to get *Aadhaar* numbers for a few hundred rupees in LP indication, most Indians appear to be a lot less concerned about the safety of their personal data in the government's hands than privacy advocates would have us believe. People seem willing to push the privacy boundary farther away than we could have ever imagined just a few years back, even with private agencies, in return for day-to-day conveniences.

Be that as it may, with the explosive growth in e-Commerce and mobile telephony, and over five years of on-the-ground experience with *Aadhaar*, I believe that India is now in a much better position to take on the challenge of creating a comprehensive data security/data privacy law. Perhaps, the *Aadhaar* Law can serve as a starting point for such an exercise. If we move decisively in that direction, there is no reason why *Aadhaar* can't be implemented more widely without unduly compromising privacy.

As for the *Aadhaar* Law, some commentators have noted that it has stronger privacy provisions than the original draft of 2010 by the UPA (United Progressive Alliance) government, while others have noted that the Law is not specific enough in some areas to address privacy concerns. My own view is that greater care could have been taken to ensure that the language in the Law did not leave room for second-guessing the government's intent or to give credence to certain nightmare scenarios.

For example:

1. The catchall phrase "*…or such other biological attributes of an individual as may be specified by regulations,"* has understandably raised alarm that it could allow collection of DNA data in the future without the consent of the Parliament.

Perhaps, this is only a provision for adopting better biometrics in the future as technology evolves. And the government might argue that there is no reason for alarm as any addition to the scope of data collection would have to be covered by Aadhaar Regulations, which would have to be placed in front of the Parliament anyway. But would it not have been wiser to explicitly prohibit the collection of DNA under the Law to head off such a serious privacy concern?

2. The last part of the clause "The Authority shall respond to an authentication query with a positive, negative or any other appropriate response…" is seen by some as walking-back from UIDAI's oft-stated "black box" explanation that the only response to authentication requests will be a Yes or No.

If the intent behind "any other appropriate response" were to allow for other responses, say, OTP (One time Password), or qualifiers to a 'No' response, etc., then UIDAI would do well to explain such intent clearly in the upcoming Aadhaar Regulations.

3. The clause "*No court shall take cognizance of any offence punishable under this Act, save on a complaint made by the Authority…"* has raised some questions about potential conflict of interest.

It seems to me that this clause pertains only to crimes as defined in the *Aadhaar* Law, such as data breaches, impersonations, etc., and it does not seem to preclude legal recourse to a resident on other matters pertaining to UIDAI and *Aadhaar*. If so, the government would do well to clear the air on this legitimate concern.

Let me conclude by referring to the debate on the clause in the *Aadhaar* Law that refers to the use of *Aadhaar* by private agencies: example, a write-up in The Hindu posited that this clause contradicts the stated objectives of the Law. Far from it, I believe that the boundaries between government and private agencies are becoming increasingly blurred even in the matter of managing government subsidies, and the incremental benefits of *Aadhaar* especially to the middle class is much more likely to come from various applications being developed by the private sector. So, it is only appropriate that the Law does not limit the use of *Aadhaar* just to government agencies. However, this only makes the matter of a comprehensive data security/protection legislation, covering both the government and the private sector, that much more urgent.