Observations on the People's Tribunal on Aadhaar-related issues held on February 29 and March 1, 2020 in New Delhi

Subhashis Banerjee

Computer Science and Engineering
(also associated with the School of Public Policy)

IIT Delhi

March 3, 2020

1. Exclusion to basic rights in welfare - including to food, employment, social security pensions, education, mid-day meals, maternity benefits, hospital treatment and other health care needs etc. - is undoubtedly the most unacceptable aspect of Aadhaar.

2. Aadhaar has a clear theory of exclusion due to Aadhaar-based biometric authentication (ABBA)[1]. The exception handling is poorly and ambiguously specified, and is hence unsound. In view of this, biometric authentication for welfare disbursal clearly fails the proportionality test and is hence unconstitutional.

3. Unlike ABBA, which is an inalienable property of Aadhaar, some of the other causes of exclusion, indignity and violation of rights in the larger Aadhaar ecosystem of service delivery are avoidable. Some examples are linking errors and missing family members in PDS rolls[2,3]; linking and exclusion errors in social security pensions[2], NREGA and DBT[2,4]; errors in NREGA muster roles[4]; incomplete use cases leading to vague errors like "inactive Aadhaar" in NPCI[4,5]; poorly thought out use cases affecting gender rights[6] - like arbitrariness in recording of gender and addresses[7], and in demanding Aadhaar for hospital treatments and medical termination of pregnancy[8] - causing Aadhaar update errors[9] and forcing old people to travel unreasonable distances to access banking[2]; extra-statutory and poorly thought out use cases in FinTech[10] and de-duplication of voter lists[11] . Many of these are indicative of poor process design and audit not limited to Aadhaar. Fixing these may not only require replacement of whole or parts of the Aadhaar ecosystem, but will also require interrogation of systems and processes beyond Aadhaar.

[1] Deposition by Anand Venkatanarayanan; with the small caveat that biometric authentication is usually a classification based on a threshold score, which may or may not admit a probability interpretation
[2] Deposition by Nikhil Dey
[3] Depositions by Aditi, Neeraj, Sameet Panda and Sachin Jain
[4] Depositions by Sakina Dhorajiwala and Rajendran Narayanan
[5] Deposition by James Herenj
[6] Deposition by Sweta Dash
[7] Deposition by Meera
[8] Deposition by Deepa
[9] Several depositions
[10] Deposition by Anivar Aravind
[11] Depositions by Srinivas Kodali and Prasanna S

4. Apart from exclusion, perhaps the direst aspect of Aadhaar is the non-federal, non-social definition of digital identity by an opaque, centralised bureaucracy (distinct from centralised storage). The definition forces one to establish and update one's identity - at least insofar as conducting business with the government is concerned - at UIDAI windows. This is bound to diminish individual control over one's identity making satisfactory grievance redressal difficult, if not impossible. It seems inevitable that this centralisation of identity definition will lead to indignity and exclusion, impacting all Article 21 rights, as is evident from the depositions highlighting gender identity problems[12]. However, the identity definition conundrum was somehow not examined adequately in the tribunal.

5. Several deponents[13,14] drew attention to the potential harm that may arise out of seeding multiple national databases with unique Aadhaar identifiers, often without any statutory backing. It is undeniable that this can create an architecture for state surveillance which can be a major threat to civil liberty and democracy. Such reckless linking of databases[15] without adequate safeguards violates fundamental rights in several ways[14], and a much more careful analysis of this was required in the majority opinion in Supreme Court's Aadhaar judgment.

   However, it appears that the linking issue is more nuanced. If the state has a responsibility for service delivery to citizens, then it may sometime need to understand them from multiple perspectives, and there may be a legitimate state aim in linking siloed databases for "real-time governance"[15].

   Moreover, it is not obvious that siloed databases without Aadhaar seeding preserve privacy significantly better than if they are seeded with an identifier like Aadhaar. There are several theoretical results to suggest that in presence of arbitrary auxiliary information - as may be available from newspapers and the internet - there can be no bounds on privacy losses under inferential attacks to privacy if there is unrestricted access to these siloed databases. Consequently, there can be no guarantees against de-anonymisation and discovery of personal identifiable information. In fact, using virtual identifiers in public databases instead of any traditional personal identifiers - like names and addresses, for example - is decidedly more privacy preserving, and unrestricted accesses to these databases always entail privacy risks. The access control problem becomes exacerbated with the frequent data leaks[16]. With increasing digitisation requirements of the state, design of safe and purpose-limited linking of siloed databases remain an important open problem, both technically and legally.

6. Poor security in Aadhaar, as is evident from multiple episodes of data leaks[16], is a serious cause of concern. Any security breach in such a crucial data ecosystem entails serious privacy risks. While it is true that many of the leaks have happened from peripheral systems, and not through direct attacks on the central repository, UIDAI - as the designer of the overall architecture - cannot absolve itself of the blame. Dismissing every data leak episode with statements like "but the central database is safe" is pointless denial that serves no purpose. The UIDAI needs to engage much more proactively with the users and civil society regarding bug reports and error handling. The Aadhaar security architecture should also be publicly audited.

[12] Depositions by Sweta Dash and Meera
[13] Deposition by Srinivas Kodali
[14] Deposition by Ujwala Uppaluri
[15] In particular, the state resident data hubs (SRDHs) described in Srinivas Kodali's deposition
[16] Deposition by Karan Saini. Written deposition by Sandeep Shukla

7. It appears that there were several anomalies in Supreme Court's handling of the Aadhaar case[17]. Not only was most of the exclusion related evidence submitted by the petitioners ignored, but the petitioner's request for oral depositions by experts with possible subsequent cross-examinations was also turned down. However, the CEO of UIDAI was allowed to make an informal presentation to the court, which seems to have affected the majority decision significantly. The majority opinion ignored the exclusionary properties inalienable to biometric authentication without adequate analysis, and accepted the government's assurance that exception handling methods will be put in place to ensure that nobody is excluded from their entitlements. The court failed to note that with mandatory biometric authentication it is impossible to separate the true negatives from the false negatives, and, consequently, any exception handling is bound to be unsound[18].

   The applications of the proportionality test - both for biometric authentication and for privacy violation - appear to be incomplete[17,19]. Moreover, while the majority opinion decided that Aadhaar failed the proportionality test for privacy for all other applications, it allowed the use of Aadhaar for disbursal of welfare. Thereby, it almost suggested by implication that privacy of welfare beneficiaries is of lesser consequence.

   It also appears that the majority judgment's acceptance of passing of the Aadhaar Act as a money bill is deeply flawed[20].

8. When it comes to legislating applications of technology, it appears that both the processes and the outcomes are far from satisfactory[21]. This is evident not only in the Aadhaar Act and its amendments, but also in the draft data protection bills - both in the original version proposed by the committee headed by Justice B N Srikrishna, and in the one presented in the parliament.

   The parliamentary processes followed for passing the Aadhaar Act leaves much to be desired. Whereas an earlier version was critiqued by a standing committee of the parliament, there was no public consultation on the version that was finally passed in 2016 as a money bill. It was not even adequately discussed in the parliament. The amendments that have been brought about in the Aadhaar Act after the Supreme Court judgment on Aadhaar were introduced as an ordinance in 2019, which definitely is not the best-practice to make amendments to controversial provisions in a disputed Act.

   Both versions of the data protection bill fail to adequately deal with the complex topic and are unlikely to be effective. This is less than satisfactory, considering that much of the privacy concerns that have emerged in the context of Aadhaar actually extend well beyond Aadhaar. Threats to individual privacy and civil liberty is a function not only of Aadhaar but also of all other digitisation efforts, in both the government and the private sector. Only an effective data protection framework can mitigate or contain the risks.

[17] Deposition by Vrinda Bhandari
[18] Deposition by Usha Ramanathan
[19] Written deposition by Gautam Bhatia.
[20] Deposition by Abhishek Jebaraj
[21] Depositions by Raman Chima and Apar Gupta