Where goes Aadhaar?

Subhashis Banerjee

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

IIT Delhi

July 14, 2019

The Aadhaar amendment bill, which provides for voluntary use of Aadhaar for KYC under the Telegraph and the Prevention of Money Laundering Acts, has now been passed by both houses of the parliament. It has reinstated many of the provisions of the Section 57 of the original Aadhaar Act which was struck down by the Supreme Court in September 2018 as unconstitutional. Considering that Aadhaar virtual identities and offline authentication were introduced well before the judgment, the amendment comes with no major alteration in either design or use cases. Aadhaar undoubtedly is a technical and administrative achievement of an unprecedented scale, and KYC has been one of its more successful use cases. However, the steamrolling of the legislative processes, without heed to the Supreme Court judgment or civil society concerns, appears to be closed-minded and brazen. Such disregard of dissenting opinions by planners and policy-makers is a definite cause of disquiet.

Section 57 was struck down not only because of the procedural issue of passing Aadhaar as a money bill, but also due to serious concerns related to privacy and proportionality. Moreover, the dissenting judgment of Justice Chandrachud found many other aspects of Aadhaar objectionable, including biometric authentication, and declared it to be unconstitutional in its entirety. In fact, very recently the Supreme Court of Jamaica has also unanimously struck down their very similar National Identification and Registration Act as completely unconstitutional by heavily relying upon and extensively citing the dissenting opinion of Justice Chandrachud. Clearly, there are several aspects of the Aadhaar technical design and its use cases that require serious reconsideration.

Mandatory deployment of biometric authentication for everyday transactions in sectors like welfare, with no clear protocol for demarcating the false negatives from the true negatives, inevitably causes denial of service for some. The requirement of reliable online connectivity compounds the problem. While this gives Aadhaar a clear theory of exclusion, its theories of inclusion and efficiency in welfare are not adequately developed. Obviously, a lot more than Aadhaar need to be in place to empower citizens to receive their entitlements.

A nation-wide digital identity limited only for de-duplication, authentication, KYC and limited fintech services is rather narrow. The Aadhaar design did not envisage using it for building online social, financial and asset registries, electronic health records etc. Consequently, the instrument lacks the robustness and privacy safeguards necessary to support such applications. The design also did not examine safe protocols for facilitating analytics for targeting for welfare, education and healthcare, econometric analysis, epidemiological studies, tax compliance etc., as the recent economic survey has suggested. This resulted in overreach with a narrow design, and ad hoc and extralegal Aadhaar seeding in registries like the State Resident Data Hubs (SRDHs), which ultimately had to be discontinued. Commercial use of Aadhaar linked data, also proposed in the recent economic survey, raises yet another set of very serious legal and technical questions.

The privacy attack surface in Aadhaar is inadequately modelled. There is no clear analysis of the minimum information that needs to be exchanged during authentication and KYC for various applications. Also, using the same identity across multiple applications may allow correlation of identities across domains and illegal profiling, and the voluntary-only use of virtual identities does not entirely mitigate the problem. Tracking and identification without consent may also happen through accessing the Aadhaar database and the authentication logs without legal sanctions. Moreover, because biometrics are not secret information, Aadhaar is vulnerable to illegal harvesting of biometrics, identity thefts and other frauds. The limited use of Aadhaar in welfare and KYC for phone and banking does not differentially add to the privacy risks of illegal profiling, because these databases can be linked even without Aadhaar. However, with the expanding scope and registries such as the SRDHs, the privacy risks are considerable.

Lack of protection against insider threats, lack of clear policies on use of virtual identities - especially on how the already linked Aadhaar information may be replaced, and whether or not only virtual identities will be linked henceforth - and lack of any regulatory oversight and a data protection law raise some serious privacy concerns. As many have pointed out, the inadequate privacy safeguards can potentially give the government of the day unprecedented access to information and power over its citizens threatening civil liberty and democracy.

Also, Aadhaar does not record the purpose of authentication. Authentication without authorisation and accounting puts users at serious risks of frauds because authentication or KYC meant for one purpose may be used for another, and there have indeed been such instances. Recording the purpose of authentication is crucial, even for offline use. Privacy-by-design is not achieved by self-imposed blindness.

And, despite repeated demands from the civil society, there still is no publicly available comprehensive audit of either the enrolment process and the de-duplication efficacy, or of the exclusion rate due to Aadhaar.

It is also becoming evident that a non-social, non-federal definition of identity by an opaque centralised bureaucracy is ill suited for delivery of welfare services which are federated state responsibilities. Neither the Aadhaar holders nor the agencies responsible for service delivery have any control over either identity or authentication, causing understanding gaps and making grievance redressal difficult.

The way forward seems to be through transparency, regular design reviews and use case audits, and a reliable and confidence building process of public consultations. Thoughtful design of a federated and de-duplicated digital identity with provable privacy guarantees from which multiple application specific virtual identities can be derived in a self-sovereign manner, which can support large scale registries and analytics by the government, and which does not take away agency from the users during authentication and authorisation, is still very much an open problem.