

Privacy concerns with Aadhaar

Subhashis Banerjee Subodh Sharma

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

IIT Delhi

June 5, 2019

The debate engendered by the Aadhaar project has propelled us from being a predominantly pre-privacy society to one in which privacy protection in digital databases has emerged as a major national concern. The welcome and scholarly Supreme Court judgment [9] has upheld privacy as a fundamental right, and informational self-determination and the autonomy of an individual in controlling usage of personal data have emerged as central themes across the judgment.

The main privacy concerns with Aadhaar are [1]:

Identity theft: Aadhaar is vulnerable to illegal harvesting of biometrics and identity frauds because biometrics are not secret information [11, 4]. Moreover, possible leakage of biometric and demographic data, either from the central Aadhaar repository or from a point-of-sale or an enrolment device, adds to the risk.

Identification without consent using Aadhaar data: There may be unauthorised use of biometrics to identify people illegally. Such violations may include identifying people by inappropriate matching of fingerprint or iris scans or facial photographs stored in the Aadhaar database, or using the demographic data to identify people without their consent and beyond legal provisions.

Correlation of identities across domains: It may become possible to track an individual's activities across multiple domains of service using their global Aadhaar IDs which are valid across these domains. This would lead to identification without consent.

Illegal tracking of individuals: Individuals may be tracked or put under surveillance without proper authorisation or legal sanction using the authentication and identification records and trails in the Aadhaar database, or in one or more authentication requesting agencies databases. Such records may reveal information on location, time, and context of authentication and the services availed.

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 [6]. Recording the purpose of authentication is crucial, even for offline use [2]. Privacy-by-design is not achieved by self-imposed blindness.

Lack of protection against insider threats and lack of virtual identities - which were retrofitted in a limited way [10] - raise some serious privacy concerns, and the absence of a clear data usage policy and regulatory oversight exacerbates the problem [1]. Without a robust consent and purpose

limitation framework and a regulatory access control architecture, the privacy concerns will remain. 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 [3, 5, 8].

The Supreme Court's three-pronged proportionality test for the constitutionality of Aadhaar was based on determination of a 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 [8]. Although the majority judgment upheld the constitutionality of Aadhaar, it struck down most of its uses on privacy grounds and limited its scope to only disbursement of welfare and income tax. The dissenting minority judgment however found Aadhaar to be unconstitutional in its entirety. Moreover, the Supreme Court of Jamaica has also recently struck down their very similar Jamaican National Identification and Registration Act (NIRA) as unconstitutional by heavily relying upon and extensively citing the dissenting Aadhaar judgment [7]. Judicious design of a national identity system that is respectful of fundamental rights is still very much an open problem.

References

- [1] Shweta Agrawal, Subhashis Banerjee, and Subodh Sharma. Privacy and Security of Aadhaar: A Computer Science Perspective. *Economic and Political Weekly*, Vol. 52(Issue No. 37), 16 2017.
- [2] Subhashis Banerjee and Subodh V. Sharma. An offline alternative for Aadhaar-based biometric authentication. <https://www.ideasforindia.in/topics/productivity-innovation/an-offline-alternative-for-aadhaar-based-biometric-authentication.html>, 2018. [Online; posted 24-September-2018].
- [3] Jean Dréze. The Aadhaar coup. <http://www.thehindu.com/opinion/lead/jean-dreze-on-aadhaar-mass-surveillance-data-collection/article8352912.ece>, 2016. [Online; posted 15-March-2016].
- [4] Rachna Khaira. Rs 500, 10 minutes, and you have access to billion Aadhaar details. <https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>, 2018. [Online; posted 4-January-2018].
- [5] Reetika Khera. *Dissent on Aadhaar: Big Data Meets Big Brother*. Orient BlackSwan, 2019. Edited volume.
- [6] PTI. UIDAI suspends Airtel, Airtel Payments Bank's e-KYC licence over Aadhaar misuse. <https://economictimes.indiatimes.com/news/politics-and-nation/uidai-suspends-airtel-airtel-payments-banks-e-kyc-licence-over-aadhaar-misuse/articleshow/62096832.cms>, December 2017. [Online; posted 16-December-2017].
- [7] Justice Bryan Sykes, Justice David Batts, and Justice Lisa Palmer Hamilton. In the Supreme Court of Judicature of Jamaica, Claim No. 2018HCV01788 Between JULIAN J ROBINSON and THE ATTORNEY GENERAL OF JAMAICA. [http://supremecourt.gov.jm/sites/default/files/judgments/Robinson%](http://supremecourt.gov.jm/sites/default/files/judgments/Robinson%20v%20Attorney%20General%20of%20Jamaica.pdf)

[2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf](#), 2019. [Online; Accessed May 23, 2019].

- [8] K S Puttaswamy and Another v Union of India (2018): Writ Petition (Civil) No 494 of 2012, Supreme Court judgment dated 26 September. https://www.supremecourtsofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf, 2018. [Accessed March 29, 2019].
- [9] K S Puttaswamy v Union of India (2017): Writ Petition (Civil) No 494 of 2012, Supreme Court judgment dated 24 August, 2017. [Accessed January 9, 2018].
- [10] Subodh Sharma (via Pratap Vikram Singh). Virtual ID is a good beginning; much more remains to be done. <http://www.governancenow.com/views/interview/virtual-id-is-a-good-beginning-much-more-remains-to-be-done>, 2018. [Online; posted 16-January-2018].
- [11] L. Viswanath. Four Reasons You Should Worry About Aadhaar's Use of Biometrics. <https://thewire.in/featured/real-problem-aadhaar-lies-biometrics>, 2017. [Online; posted 28-March-2017].