Aadhaar needs a privacy law

The Supreme Court's (SC's) landmark judgement upholding our right to privacy has intensified the debate on whether and how Aadhaar infringes on this right. With the upcoming five-judge Constitution bench hearing petitions on Aadhaar, these debates will soon be settled by the highest court.

Meanwhile, the Unique Identification Authority of India (UIDAI) has unequivocally asserted that Aadhaar meets the privacy test. But many others, both within the government's fold and outside it, have said that Aadhaar can become an instrument to profile individuals, surveil them, and suppress dissent.

The boring but important truth is that both sides are right—to some degree. Aadhaar, if unregulated, can be a tool to abrogate our privacy. However, Aadhaar is only a tool. Other tools of the government—such as CCTV cameras, permanent account number (PAN) cards, Digital India, among others—are also capable of invading privacy. When dispassionately analysed, each of these tools, including Aadhaar, meet some, but not all, principles of adequate data privacy.

The solution, therefore, is not to annul Aadhaar on the grounds of data privacy. Like we do with any tool in the public domain, we need to avail of its benefits and manage the risks, while evaluating whether the benefits are worth the risks. To this end, we need two parallel initiatives to complement the court's decisions.

One, rigorous, and independent research such as the Indian School of Business' digital ID research initiative is vital to ascertain the benefits and risks across Aadhaar's uses. This can help decide which uses should be furthered, adjusted, or even dropped. This is critical because Aadhaar's uses are proliferating, but most of the available numbers on its impact are disputed and alternative narratives are based on journalistic accounts or small surveys. Two, we need an independent regulator to protect data privacy and regulate data initiatives (as argued in the data privacy Bill introduced by Baijayant Panda). This regulator must be backed by a robust law, and be competent to understand the nuances of data privacy and keep pace with new developments. This is urgent. We are many strides into a digital economy and are already suffering the consequences of this void.

cracIAS.com

Debate on Aadhaar and privacy has largely reached an impasse as those involved often use different definitions of data privacy. This can be avoided by the universal adoption of National Privacy Principles. Aadhaar is often analysed in a vacuum, without paying enough attention to national benchmarks (such as PAN, voter ID, passport, etc.). In this article, we examine data privacy issues with these factors in mind.

One potential harmful abuse of Aadhaar is using the unique number to link data sets that previously existed in silos. Depending on the breadth of data sets seeded with Aadhaar, they can be merged to uncover a person's "food habits, language, health, hobbies, sexual preferences, friendships, ways of dress, and political affiliation", as the SC worried in its judgement on right to privacy. Not only is this objectionable in and of itself, such profiling can be used to discriminate against individuals and stifle dissent.

Aadhaar is not the only unique identifier in our lives that can be used to link databases. Our mobile numbers, email addresses, PAN, voter ID, ATM card numbers and IP addresses can all serve this purpose (and indeed have).

Four features, however, make Aadhaar particularly potent for database linking. One, it covers

almost all Indian adults. Two, the database has practically no duplicates (according to UIDAI), enabling a higher quality of linking. Three, it uses a 12-digit unique identifier, making linking easy. Four, over 120 government agencies require Aadhaar to provide services, paving the way for the first step of data linking—seeding each individual database with Aadhaar numbers. The irony is that the quality of the Aadhaar database (the first three reasons) leads to its widespread use (the fourth reason), making it susceptible to misuse.

Unauthorized database-linking violates almost all the National Privacy Principles, including "Purpose Limitation", whereby "a data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals."

An operative phrase here is "data controller". UIDAI's chief executive officer, Ajay Bhushan Pandey, recently reaffirmed that Aadhaar meets the principle of Purpose Limitation. He is partially right: while Aadhaar can be used for database linking, UIDAI as a "data controller" does not engage in this practice (though it cannot prevent it either). However, other "data controllers" (say, criminal investigation agencies or credit card companies) with access to data-sets seeded with unique identifiers, such as Aadhaar, can link databases without due notice or consent and use it nefariously.

Therefore, attacking only Aadhaar for the larger privacy risk of database linking is not based on a practical understanding of how linking works. Aadhaar is only the means to an end. If Aadhaar ceased to exist, the threat of database linking using unique identifiers will endure, albeit with higher difficulty. This reinforces the need for a strong data privacy law and regulator to curb and manage database-linking practices.

Ronald Abraham is a partner at IDinsight and co-author of State of Aadhaar Report 2016-17

Research contributions from Shreya Dubey and Akash Pattanayak. This is the first of a two-part series on Aadhaar and privacy.

Comments are welcome at theirview@livemint.com

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com