AADHAAR

TIMES OF INDIA, Delhi, 2.3.2018

Page No. 16, Size:(20.29)cms X (18.92)cms.

What Aadhaar Collects

Fears of a surveillance state are overblown, but a robust privacy bill is needed

Srikanth Nadhamuni

Claims, insinuations and even jokes have done the rounds on print and social media about how the Aadhaar system could lead to a surveillance state. There are worries that unsuspecting Aadhaar carrying residents will be closely tracked by the government while they authenticate themselves as they pay for their pizza or buy rice at a ration shop.

We need to understand what data Aadhaar collects and more importantly what it doesn't, to determine whether the above dystopian scenarios are likely or even possible.

Aadhaar does only two things. First, enrolment, wherein an applicant is processed and issued an Aadhaar number. Second, online authentication where the Aadhaar holder is accurately verified during a transaction such as buying rations.

Back in December 2009, a government appointed committee with representatives from several ministries, regulators and NGOs met to determine which demographic fields should be collected to issue an Aadhaar. After lengthy deliberations, the committee came up with a simple rule – UIDAI should only collect the minimal amount of information in order to protect the privacy of the people. The four mandatory fields were, 'Name', 'Address', 'Gender' and 'Date-of-birth'. 'Email' and 'mobile number' were left optional.

Similarly, a government appointed biometric committee decided that ten fingerprints, two irises, and a photo of the face were needed to accurately de-duplicate the entire population and issue a unique ID, thus ensuring that a resident does not get multiple Aadhaar IDs. This was the bane of earlier systems, where programme-based ID cards which lacked uniqueness (one person, one ID) resulted in duplicates and ghost IDs, leading to resource capture, leakage and other fraudulent transactions.

Based on the above demographic and biometric data that is collected, the enrolment system issues an Aadhaar number after a de-duplication process to ensure that the resident is unique and does not already possess an Aadhaar number.

Once the resident is enrolled in the Aadhaar system, she can now authenticate herself at various points to prove her identity. Just as one would enter a user-ID and password to login to one's email account, the Aadhaar holder can now authenticate herself by entering her Aadhaar-number (user-ID) and one of the demographic/ biometric details (password). This online verification proves to be very useful in a host of services, be it government service delivery, banking/ payments or even renting a bicycle.

Now let's look at Aadhaar authentication.

During authentication, the user enters the Aadhaar number and one or more of the biometric (fingerprint/ iris) or demographic (name/ address/ gender/ date of birth) fields and Aadhaar returns a Yes/ No response. It does not return other details about the person, hence protecting the privacy of the individual.

Over 75% of smartphone users enable location services. In contrast, the Aadhaar authentication system is designed to protect people's privacy by not collecting such information

The Aadhaar system does not collect the specific purpose of your authentication, or the location of your transaction so there is no way the system can construct where you were and what you were doing. As can be seen in Section 3.3 of the 'Aadhaar Authentication API Specification', there is no input field in the data format that collects the location or type of transaction being carried out (example, paying for your pizza or buying rice at a ration shop).

Delving deeper into privacy and accountability, let's look at the audit trail feature Aadhaar provides so that you can view your Aadhaar transactions and ensure that they were all bonafide– just as you reconcile your bank statements. It can be argued that if the history of Aadhaar transactions contained details such as *what* (specific transaction type), *where* (location information) and by *whom* (authenticating entity), the user would be empowered with context against potential frauds by more accountability in the system. In fact, an earlier version of the Authentication API spec did collect the location information for this very reason. On the contrary, it can also be argued that collecting the *where* and *what* and *who* would compromise the Aadhaar holder's privacy.

The point i'm making is that a line has to be drawn somewhere between privacy and accountability and you can't have both independent of each other. A measured, balanced approach between the two is in the interest of citizens and this, i believe, is what Aadhaar offers.

An average smartphone user can be tracked by the telecom provider who can triangulate the user's location through telecom base stations. Apps from Google, Facebook, Apple and thousands of other companies are also able to track smartphone user location using GPS sensors. Surveys show that over 75% of smartphone users enable location services. This is the reality of the digital world we live in. In contrast, the Aadhaar authentication system is designed to protect people's privacy by not collecting such information.

India is coming to terms with privacy in this increasingly digital world for the first time. The debate around Aadhaar privacy is a precursor to the larger privacy debate. It is a good thing that people are becoming aware of the issues around privacy.

Aadhaar brings tremendous benefits to our country, be it in plugging the leaky pipes of the government's benefits delivery, or convenient pension payments. The passing of a robust privacy bill and Aadhaar compliance to it would hopefully help alleviate concerns as we strive to build systems of better service delivery in a data rich and digital India.

The writer was founding head-of-technology of the Aadhaar project