Aadhaar hasn't fixed identity fraud, it's made it worse

Pranesh Prakash

2018-01-05

The Quint

Abstract

UIDAI has been providing access to people's identity information without their knowledge or authorisation.

Debate around Aadhaar is missing the point about whether people know how to intervene in case of data breach.

A recent report in the *Tribune* ('Rs 500, 10 minutes, and you have access to billion Aadhaar details') points to vulnerabilities in the Aadhaar ecosystem. By paying an anonymous tout Rs 500, a journalist was about to access demographic details of Aadhaar number holders by entering an Aadhaar number.

The Unique Identification Authority Of India (UIDAI) has called this "misreporting" and has stated that no biometric information has been leaked and there has been "no biometric data breach".

The UIDAI's reponse is a non-response since the *Tribune* article doesn't claim that any biometric information was breached. Further, if we take it to be a fact that the UIDAI's systems didn't have to be breached, then that itself points to a severe problem: that people who (legitimately) have access to Aadhaar-linked data are selling such access.

As the Twitter handle @Databaazi has been pointing out for some time, there is a little-known feature called the DBT Seeding Data Viewer (DSDV), which provides full access to all Aadhaar-linked demographic data to thousands of government officials without seeking the consent of the people whose data is visible.

Furthermore, the UIDAI's handbook for enrollment agencies allows them to retain all the data that UID applicants have submitted, including the biometrics.

We should also keep in mind that the systems mandated by the government before Aadhaar (identification photocopies for know-your-customer forms, for instance) also provided ample scope for unauthorised access and use, and indeed there were and continue to be secondary markets for these identification details, including phone numbers, which can be used for identity fraud. Aadhaar, we were promised, would fix that.

> It is now clear that Aadhaar doesn't fix that problem, and in fact makes the problem worse by centralising identity data, which were disaggregated earlier among various photocopy shops and mobile phone stores.

The UIDAI has admitted that it has revoked the licences of 49,000 enrollment agencies, for a variety of reasons, including corrupt practices, but that leaves unclear what happened to the data that was collected by those agencies.

What should worry us is that the UID ecosystem (which is distinct from UIDAI) is leaking like a sieve, even when UIDAI's databases are secure. If a 'legitimate' party who has access to the Aadhaar database (which can be procured even through entities other than UIDAI, such as each state's Resident Data Hubs), is illegitimately selling access, then it is almost impossible to detect, since the unscrupulous use will be almost indistinguishable from the expected use. Clearly, UIDAI is failing in its duty, provided under Section 28 of the Aadhaar Act, to "ensure confidentiality of identity information ... of individuals".

> UIDAI has been providing access to people's identity information, without the knowledge or authorisation of individuals.

Thus, to prevent this kind of illegitimate access to people's data, UIDAI has to ensure that no entity — governmental or otherwise — has access to an individual's Aadhaar-linked information without the individual's express authorisation.

Ask yourself: Did you consent to copies of the data that you submit to UIDAI being provided to any third parties for inclusion in State Data Resident Hubs or for access through systems like DSDV? Had you even heard these terms before?

Fixing this means that, at a minimum, State Resident Data Hubs need to be shut down, that all "inorganic" seeding of Aadhaar number (that is, adding your Aadhaar number to a database without your express permission) done to date needs to be undone, and that the kinds of access that DBT Seeding Data Viewer provides needs to be removed.

Lastly, we need clear legal restrictions on when Aadhaar can be used, as well as guidelines for appropriate Aadhaar use, as most instances of Aadhaar usage that we have are inappropriate. For instance, on Thursday the Karnataka government announced that all autos in Bengaluru will have to get new e-permits which are Aadhaar-linked. Why? Because they noticed that auto drivers were driving without permits and that some were driving using fake permits (that is, printed permits that resemble real permits, but aren't). Will linkage to Aadhaar prevent either of these two from happening? No, since neither of these two are instances of identity fraud. Indeed, it is easy to simply "print" an Aadhaar card with any details, as Azam Khan in Madhya Pradesh did for his dog Tommy Singh.

> Linkage to Aadhaar doesn't magically fix fraud, but increased checking of permits by the traffic police along with real-time checking of permit number in a database might.

This is just one example. Most instances of Aadhaar linkage are similarly pointless since they don't help solve anything and can be done more easily without Aadhaar. Given its in-depth knowledge, the UIDAI should guide government officials as to what Aadhaar can do and cannot do, rather than overselling the questionable potential benefits of Aadhaar.

(*Pranesh Prakash is Policy Director at Centre for Internet and Society. This article was originally published in* BloombergQuint*, and has been republished with permission.*)