Aadhaar marks a fundamental shift in citizen-state relations: from "We the people" to "We the government"

Pranesh Prakash

2017-04-01

Hindustan Times

Abstract

Your fingerprints, iris scans, details of where you shop. Compulsory Aadhaar means all this data is out there. And it's still not clear who can view or use it

---

Imagine you're walking down the street and you point the camera on your phone at a crowd of people in front of you. An app superimposes on each person's face a partially-redacted name, date of birth, address, whether she's undergone police verification, and, of course, an obscured Aadhaar number.

OnGrid, a company that bills itself as a "trust platform" and offers "to deliver verifications and background checks", used that very imagery in an advertisement last month. Its website notes that "As per Government regulations, it is mandatory to take consent of the individual while using OnGrid", but that is a legal requirement, not a technical one.

Since every instance of use of Aadhaar for authentication or for financial transactions leaves behind logs in the Unique Identification Authority of India's (UIDAI) databases, the government can potentially have very detailed information about everything from the your medical purchases to your use of video-chatting software. The space for digital identities as divorced from legal identities gets removed. Clearly, Aadhaar has immense potential for profiling and surveillance. Our only defence: law that is weak at best and non-existent at worst.

The Aadhaar Act and Rules don't limit the information that can be gathered from you by the enrolling agency; it doesn't limit how Aadhaar can be used by third parties (a process called 'seeding') if they haven't gathered their data from UIDAI; it doesn't require your consent before third parties use your Aadhaar number to collate records about you (eg, a drug manufacturer buying data from various pharmacies, and creating profiles using Aadhaar).

It even allows your biometrics to be shared if it is "in the interest of national security". The law offers provisions for UIDAI to file cases (eg, for multiple

enrollments), but it doesn't allow citizens to file a case against private parties or the government for misuse of Aadhaar or identity fraud, or data breach.

It is also clear that the government opposes any privacy-related improvements to the law. After debating the Aadhaar Bill in March 2016, the Rajya Sabha passed an amendment by MP Jairam Ramesh that allowed people to opt out of Aadhaar, and withdraw their consent to UIDAI storing their data, if they had other means of proving their identity (thus allowing Aadhaar to remain an enabler).

But that amendment, as with all amendments passed in the Rajya Sabha, was rejected by the Lok Sabha, allowing the government to make Aadhaar mandatory, and depriving citizens of consent. While the Aadhaar Act requires a person's consent before collecting or using Aadhaar-provided details, it doesn't allow for the revocation of that consent.

In other countries, data security laws require that a person be notified if her data has been breached. In response to an RTI application asking whether UIDAI systems had ever been breached, the Authority responded that the information could not be disclosed for reasons of "national security".

The citizen must be transparent to the state, while the state will become more opaque to the citizen.

How did Aadhaar change?

How did Aadhaar become the behemoth it is today, with it being mandatory for hundreds of government programmes, and even software like Skype enabling support for it?

The first detailed look one had at the UID project was through an internal UIDAI document marked 'Confidential' that was leaked through WikiLeaks in November 2009. That 41-page dossier is markedly different from the 170-page 'Technology and Architecture' document that UIDAI has on its website now, but also similar in some ways.

In neither of those is the need for Aadhaar properly established. Only in November 2012 — after scholars like Reetika Khera pointed out UIDAI's fundamental misunderstanding of leakages in the welfare delivery system — was the first cost-benefit analysis commissioned, by when UIDAI had already spent 28 billion. That same month, Justice KS Puttaswamy, a retired High Court judge, filed a PIL in the Supreme Court challenging Aadhaar's constitutionality, wherein the government has argued privacy isn't a fundamental right.

> Every time you use Aadhaar, you leave behind logs in the UIDAI databases. This means that the government can potentially have very detailed information about everything from the your medical purchases to your use of video-chatting software.

Even today, whether the 'deduplication' process — using biometrics to ensure the same person can't register twice — works properly is a mystery, since UIDAI hasn't published data on this since 2012. Instead of welcoming researchers to try to find flaws in the system, UIDAI recently filed an FIR against a journalist doing so.

At least in 2009, UIDAI stated it sought to prevent anyone from "[e]ngaging in or facilitating profiling of any nature for anyone or providing information for profiling of any nature for anyone", whereas the 2014 document doesn't. As OnGrid's services show, the very profiling that the UIDAI said it would prohibit is now seen as a feature that all, including private companies, may exploit.

UID has changed in other ways too. In 2009, it was as a system that never sent out any information other than 'Yes' or 'No', which it did in response to queries like 'Is Pranesh Prakash the name attached to this UID number' or 'Is April 1, 1990 his date of birth', or 'Does this fingerprint match this UID number'.

With the addition of e-KYC (wherein UIDAI provides your demographic details to the requester) and Aadhaar-enabled payments to the plan in 2012, the fundamentals of Aadhaar changed. This has made Aadhaar less secure.

Security concerns

With Aadhaar Pay, due to be launched on April 14, a merchant will ask you to enter your Aadhaar number into her device, and then for your biometrics — typically a fingerprint, which will serve as your 'password', resulting in money transfer from your Aadhaar-linked bank account.

Basic information security theory requires that even if the identifier (username, Aadhaar number etc) is publicly known — millions of people names and Aadhaar numbers have been published on dozens of government portals — the password must be secret. That's how most logins works, that's how debit and credit cards work. How are you or UIDAI going to keep your biometrics secret?

In 2015, researchers in Carnegie Mellon captured the iris scans of a driver using car's side-view mirror from distances of up to 40 feet. In 2013, German hackers fooled Apple iOS's fingerprint sensors by replicating a fingerprint from a photo taken off a glass held by an individual. They even replicated the German Defence Minister's fingerprints from photographs she herself had put online. Your biometrics can't be kept secret.

> Typically, even if your username (in this case, Aadhaar number) is publicly known, your password must be secret. That's how most logins works, that's how debit and credit cards work. How are you or UIDAI going to keep your biometrics secret?

In the US, in a security breach of 21.5 million government employees' personnel records in 2015, 5.2 million employees' fingerprints were copied. If that breach had happened in India, those fingerprints could be used in conjunction with Aadhaar numbers not only for large-scale identity fraud, but also to steal money from people's bank accounts.

All 'passwords' should be replaceable. If your credit card gets stolen, you can block it and get a new card. If your Aadhaar number and fingerprint are leaked, you can't change it, you can't block it.

The answer for Aadhaar too is to choose not to use biometrics alone for authentication and authorisation, and to remove the centralised biometrics database. And this requires a fundamental overhaul of the UID project.

Aadhaar marks a fundamental shift in citizen-state relations: from 'We the People' to 'We the Government'. If the rampant misuse of electronic surveillance powers and wilful ignorance of the law by the state is any precedent, the future looks bleak. The only way to protect against us devolving into a total surveillance state is to improve rule of law, to strengthen our democratic institutions, and to fundamentally alter Aadhaar. Sadly, the political currents are not only not favourable, but dragging us in the opposite direction.

(Pranesh Prakash is policy director at the Centre for Internet and Society, and Affiliated Fellow at Yale Law School's Information Society Project)