

INDIA'S BIOMETRIC ID SYSTEM TRIGGERS PRIVACY LAWSUITS

The nation's Supreme Court weighs in



➤ In January, justices of the Supreme Court of India gathered to discuss the country's national identification system, called Aadhaar. Since 2010, authorities have enrolled 1.19 billion residents, or about 93 percent of India's population, in the system, which ties fingerprints, iris scans, and photos of Indian citizens to a unique 12-digit number.

Almost a decade later, India is still grappling with the technical, legal, and social challenges of launching the

world's most ambitious government identification program. Aadhaar's reach and ubiquity has made it a tempting vehicle for centralizing activity, including welfare payments and mobile number registrations. But it has also raised major privacy and security issues.

The Indian government's original argument for Aadhaar was to replace paper ration cards for food entitlements (see "India's Big Bet on Identity," *IEEE Spectrum*, March 2012). The old system excluded cit-

ID, PLEASE: A citizen presents an identification card with his Aadhaar number, which is linked to 10 fingerprints, two iris scans, and a photograph.

izens who could not obtain a card from corrupt local officials or members of families whose heads of household did not share benefits with them. Individuals, rather than households, now have Aadhaar numbers, and obtaining one is free at any enrollment office in the country.

In the years since the program began, banks, mobile operators, and the govern-

ment itself have started to require Aadhaar authentication to access services, even though India's Supreme Court has found that the government cannot force citizens to use Aadhaar to obtain entitlements.

The case now before the country's highest court, which was ongoing at press time, combines almost three dozen petitions arguing that Aadhaar violates a constitutional right to privacy and interferes with access to entitlements. While some of the petitions challenge the entire Aadhaar Act, others focus on a government requirement to use Aadhaar to verify applicants for new SIM cards or to link Aadhaar to tax IDs.

In practice, an Aadhaar number is like a telephone number: Nobody forces you to have one, but doing anything without one is almost impossible.

As Aadhaar has grown, the program has also proven susceptible to fraud. In January, *The (Chandigarh) Tribune* reported that village-level Aadhaar enrollment agents were selling access to personal details for as little as US \$8. The ability of third parties to compile such data in a central repository may be one of the weaknesses of the Aadhaar system. Days later, the Unique Identification Authority of India (UIDAI) said it would offer facial recognition along with user-generated virtual ID numbers to verify personal identities, so users would not have to reveal their Aadhaar numbers for every transaction.

When things go wrong, Aadhaar holders have limited recourse. "Individuals can't go to police to complain about compromised data, because only UIDAI can do so" under present law, says economist Reetika Khera, of the Indian Institute of Technology, in New Delhi, who has studied Aadhaar's social impact.

Many of Aadhaar's legal and social problems have their roots in incomplete technical regulations, says Jyoti Panday, Asia Policy Fellow at the Electronic Frontier Foundation, in New Delhi. "Until there is strict enforcement of the standards for collection, storage, and use of biometric data as established under the Aadhaar Act

and Regulations, these problems will keep cropping up in new ways," Panday says.

The government's relentless push to expand Aadhaar may be turning influential Indians against the program, says Khera. Now that India's middle class is being asked to link their Aadhaar to

sensitive data, they are paying more attention to mishaps. "Because the constituency has changed," Khera says, "public opinion has changed dramatically."

—LUCAS LAURSEN

[POST YOUR COMMENTS](http://spectrum.ieee.org/aadhaarid0318) at <http://spectrum.ieee.org/aadhaarid0318>