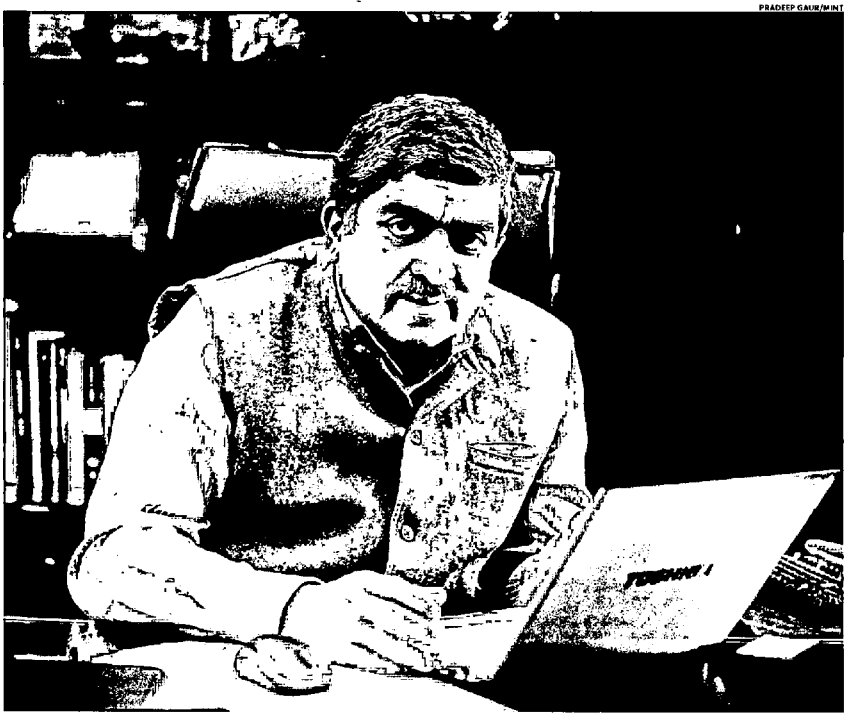
Mint Edition Delhi
5.5.2017 Page 8
Height 52.92cm Width 37.04 cm

'The biggest privacy risk that you have is your smartphone'

BY ANIRBAN SEN
feedback@livemint.com

BENGALURU

PRADEEP GAUR/MINT



The last few weeks and months have witnessed a steady stream of negative news surrounding Aadhaar, the government's unique identity number programme, with wide-ranging concerns being raised on the security of the system and the potential leakage of Aadhaar numbers by government departments. The government also received flak for making Aadhaar mandatory for filing income tax returns. Then there are issues with the technology itself—the Aadhaar biometric authentication failure rate in the rural job guarantee scheme was as high as 36% in Telangana, as reported by *Mint* in April. In an interview, Infosys co-founder and former Unique Identification Authority of India (UIDAI) chairman Nandan Nilekani, the creator of Aadhaar, dispelled most of the concerns surrounding Aadhaar, especially around the security of the system, but conceded that there are areas where it can improve, while calling for the creation of a data-protection and privacy law. Edited excerpts:

How big a problem is the current situation with the lack of a privacy law?

I'm very clear that India needs a very modern privacy and data-protection law. And I've been saying this far longer than most people. Sometime in May of 2010, I wrote to Prime Minister Manmohan Singh that we should have a privacy law. And I followed that up. I asked Rahul Matthan (partner at Trilegal and a *Mint* columnist) and he helped. He worked with the department of administrative reforms and came out with a draft law and subsequently there was a committee under Justice A.P. Shah, and one of my colleagues (at UIDAI) Ashok Pal Singh was a member of that committee. They contributed to the framing of the principles.

The only issue I have with the current narrative is, why should Aadhaar be singled out as a reason for the law? The biggest privacy risk that you have is your smartphone. A billion people will have smartphones as we go forward, their conversations will be recorded, their messages will be read, their location can be identified with the GPS or the triangulation of the towers on a real-time basis. So, for 24 hours a day, you know where a person is. Using all the accelerometers and gyrometers on the phone, you can actually make out if someone is drunk or not. The kind of intrusion of privacy that the smartphone does is order of magnitudes higher. Aadhaar is a sporadic thing—it is episodic, for instance, when I go and open an account, etc.

The second big privacy risk that we have are CCTV cameras—there doesn't seem to be a law on these things. Every mall, every retailer, every ATM, every bus-stand, every railway station, every airport, every hotel has a CCTV camera. And now, we have CCTV combined with face recognition technology.

> There's a realization that we have this extraordinary transformation in governance platform—so, there is the willingness to use this platform to achieve more

Thirdly, we have the Internet companies and data collection. Indians are essentially giving data to companies that are essentially unaccountable to Indian law and that data is often shared with foreign governments as we have seen, time and again. There is more risk of Indians sharing data with foreign governments, than their own government.

Then there are drones, or the Internet of Things, with sensors everywhere collecting data on you. So, when you look at it, there is a data tsunami that is coming due to a variety of things—(it has) nothing to do with Aadhaar as such. Given that, we should have a data-protection and privacy law which is an umbrella law, which looks at all these phenomena and certainly Aadhaar and the use of Aadhaar should be part of that.

That's perfectly fine—but people are acting as if Aadhaar is the only reason why we should have a privacy law. That's where I have a problem. We have a far bigger risk today from a cell-phone than Aadhaar.

Why are we witnessing such reluctance from the government in terms of creating this legal framework around Aadhaar?

We need to have an internal champion in the system who will take it forward. It cuts across everything. There are a lot of stakeholder interests inside the government—so, it requires someone to champion it and lead it. In any case, we need a very modern data-protection law—data generation has become so huge now; all the current constructs of data laws were designed 10-15 years ago. If you look at the work happening in Europe with the generalized data protection regulations which come into effect next year, it was actually designed pre-big data. So, how do we design it (a privacy law) so that it operates in this massive data which is coming out of sensors, phones, etc? We need to rethink the entire concept.

These (current) laws were designed for a different era.

Concerns have been raised around how Aadhaar is facilitating the creation of an Orwellian sort of surveillance state...

Again, this is another attempt to criticize and (create) this notion that Aadhaar is an instrument of mass surveillance. It's complete nonsense. Your smartphone is a much better tool for the government to do surveillance than Aadhaar. Because Aadhaar by nature is episodic. I open a bank account once in a while. I buy a SIM card once in a while. If I use it for payments, I'll use for low-value payments; I'll use other means of authentication. So, it's not really surveillance. By definition, a surveillance system is collecting data about you. The Aadhaar system does not collect data.

But there's no limit to the amount of data the system can collect on individuals...

As far as the Aadhaar system is concerned, what enters the system is very limited information and when you do an Aadhaar authentication, the Aadhaar authentication does not even know for what purpose that authentication has happened. It has been deliberately designed like that. Suppose I use it to do a financial transaction in a bank, the bank knows the financial transaction, but the Aadhaar system does not know. It's deliberately designed like that. Real surveillance happens when data is accumulated which is what is happening in many organizations and that data is a black box. Nobody knows what's happening with that data. And on top of that, you have black-box algorithms operating, which is what is happening. We have no idea what algorithms are being used today to feed you news or whatever. That is where the risks are.

What happens in the event of a data breach? Unlike a credit card, one cannot block the Aadhaar card.

I think the Aadhaar system is extremely well-designed. It's not an online system that is exposed to the Internet. When the enrolment happens, the packet is encrypted at source and sent, so that there can't be a man-in-the-middle attack. And when the authentication happens, that is also encrypted—not compared to the original data, but to a digital minutiae. The point is that the system is very, very secure. So, if the objection is to centralization, then you should not have clouds. Clouds are also centralized. Everything today is centralized—otherwise, let's all go back to pen and paper.

The point is that on Aadhaar authentication, a number of things are happening that make it even more secure because UIDAI has over the past couple of years come out with an architecture that is called registered devices. And registered devices have level-zero and level-one. Level-zero is software-based and level-one is hardware-based. Increasingly what is happening is that biometrics is now becoming common to every phone. When you're using your phone, you're giving your biometric to some company. For example, if you look at the latest Samsung Galaxy S, it has something called Fort Knox—it's a secure zone. So, secure hardware zones are now going to be standard in most of these—and this is military-grade security. So, in hardware-based registered devices, the biometric authentication details are captured and encrypted there itself. So that makes it even better and more secure. And the government or the Reserve Bank of India can say that all payment transactions should be only on level-one registered devices. So, it's a continuous game of making things more and more secure.

There's also a perception of a general lack of transparency in terms of sharing concrete data from the UIDAI on how the system has done more good than harm.

As far as I know, every RTI (request under the Right to Information law) has been responded to. But I think the Aadhaar authentication with registered devices, especially with hardware-registered devices, will make it even more safe. The Aadhaar law limits what organizations can do when they do an eKYC (electronic Know Your Customer, a process of verifying the identity of customers) with the Aadhaar number. That law has to be rigorously enforced. The Aadhaar law is a very good law—in fact, the Aadhaar law has more privacy kind of details than most laws have. But I agree we need an overall data-protection and privacy law which covers everything, including foreign companies collecting data in India, including drones, Internet of Things, people reading your emails, smartphones, etc.

But doesn't the system need to be held accountable in the event of a breach of data? That doesn't seem to be happening—for instance, a lot of things are being done in the name of national security.

Everywhere in the world national security exceptions are there. Everywhere in the world, the tension is between privacy and security because the security guys feel that if there is a criminal action, they should get access. Now, most countries do provide under national security, the ability to access very specific information—which is provided for in the Aadhaar law... I think instead of attacking Aadhaar which is a negative activity, everyone should get together and get the (privacy) law passed, which is a positive activity.

Given the developments of the past few weeks and months, is the Aadhaar law in need of an overhaul? Does the legal framework around Aadhaar need to be re-examined to ensure that the scope of the program is not abused?

The Aadhaar law which was passed in 2016 governs the UIDAI's authority, which as I said has better privacy protection than any other law that I can think of and it has a lot of checks and balances. That's one part. Then there's the use of Aadhaar which is done by other laws. For example, in the Finance Bill, they say Aadhaar should be mandatory for PAN (permanent account number) Card. That's got nothing to do with Aadhaar, that's a legal provision in another law.

There are broadly four purposes to the use of Aadhaar: first, the feature of Aadhaar, which is unique only to Aadhaar and no other system, is that it gives a unique ID across a billion people—you can be sure that somebody does not have more than one ID; second, Aadhaar is used to do direct benefit transfer by sending money to the Aadhaar number which in turn is linked to a bank where your account is; third, Aadhaar is as an online authentication system; and the fourth use of Aadhaar is as an electronic KYC where I give permission to the Aadhaar system to release my name and address to the bank and I get an instant bank account or an instant SIM card. So, four very different uses of one platform.

The first use has a used case in both benefits as well as documents. In benefits, you want to eliminate ghosts and duplicates. You want to make sure there are no fake pensioners, etc. We've already seen the value of the savings that the government has got. The government has said that the savings is somewhere around Rs49,000 crore. The total investment in Aadhaar is around Rs8,000-9,000 crore. The impact is there to be seen... a variation of the duplicate problem is in documents. India has 250 million PAN (cards). And only 40 million Indians are paying taxes. Why should there be 250 million PAN (cards) and only 40 million taxpayers? Many people have taken PAN for ID proof. But even when you discount the people who have PAN for ID, there are still many duplicate PAN (cards). The reason is that there are people who want to evade taxes. But having the Aadhaar number de-duplicate PAN numbers you're actually making sure that a guy has only one PAN number and that will help in eliminating tax evasion, so that's a good social purpose.

> Instead of attacking Aadhaar, which is a negative activity, everyone should get together and get the (privacy) law passed, which is a positive activity

Similarly, the mobile phone using Aadhaar-eKYC actually came out of a Supreme Court decision. Now, In the old days, you used to submit a copy of your passport or an ID proof, to get a SIM card. Now, that's even more unsafe—because that fellow now has all your data. Secondly, 10 other people will get a SIM using your details—you don't know.

Even though we have a billion phones, we have about 600 million unique users, is my estimate. And even in that, how many of them have given a genuine ID to get a phone? I don't know. The same story is playing out with driving licences.

But there is still concern around all this data being centralized..

No, the data is not in one system—that's the whole point. The data is in respective systems. The Aadhaar number is in the PAN database. The PAN number is not in the Aadhaar database... that's the point. The Aadhaar database does not have any data. This is a conscious design choice, which is why to say that the system is for surveillance makes no sense. The nature of surveillance requires you to collect data. This does not collect data.

But then why has Aadhaar become all-pervasive? Why is Aadhaar being made mandatory for everyone?

No, there's a realization that we have this extraordinary transformation in governance platform—so, there is the willingness to use this platform to achieve more. All the goals that we've identified are all the things that improve governance: making sure there's one PAN card reduces tax evasion; making sure that a person has done a proper KYC reduces criminality and terrorism; making sure that a person has only one driver's licence makes it easier to enforce the rules of the road, which makes it safer for you and me to travel on the roads... So everything that has been done is being done to ensure that it enhances the quality of governance. Now if the concern is of privacy, I've made my position clear.

In everything in life, there's always a trade-off between privacy and convenience. There's no absolute privacy, there's no absolute convenience. In our view, the benefits of the Aadhaar system to individuals and society far outweigh the inconvenience or the risk. Everything in life is a risk. You always see how you balance these out. But the benefits here are so huge, it's worth anything—and obviously the obligation of the Aadhaar system is to ensure that things are done properly and nobody is denied benefits. As technology evolves, you make things better and safer. Within seven years of its launch, the Aadhaar system has made a remarkable leap in terms of its security and privacy and it will keep improving. Technology does not come through immaculate conception. It has to evolve.

Speaking of evolution, what are some of things that still need to be fixed in the system?

One, I agree we need a privacy law, covering everything. Secondly, we need to implement (the concept of) registered devices as soon as possible. The first launch is by June... Also, the Aadhaar law already provides that anyone who uses the Aadhaar number cannot display the number or publish it, so that enforcement has to happen. We have to make sure that any user of this, whether it's the government or the private sector, follows the law for the protection of the Aadhaar number.

Protection of numbers and preventing leakages have been a massive issue...

I know the government has sent a notice to everyone. If somebody has done it, they ought not to have done it—there's a law for that.

Even with these kind of checks and balances, why are so many concerns being raised on the security of the system?

It's very safe. Security is an ongoing thing. You have to keep improving and getting better. You have to keep doing that and I'm sure the guys (at UIDAI) are aware of that.

The methods followed here, the architecture, the encryption, the use of HSM (hardware security module)—all these are way above what we've seen anywhere. You saw what happened with debit cards in India—there the breach happened and wasn't noticed for months. In the Aadhaar system, we've, caught these guys within 24 hours. The point is, as I said, technology will keep getting better.

Several experts on security have pointed out flaws in the system and said Aadhaar can be breached. There's also a general sense that the UIDAI is being reluctant to invite people to help improve security or point out flaws.

I want to know which government system has been as open as UIDAI has. The kind of documentation that we have put out right from day 1, design documentation, architecture documentation, standards, etc—it's incredible.

When something is built at scale, there will be points of view on that. And if there are any gaps, they have to be addressed. That's how we move forward.

But when it's a motivated campaign where the agenda is something else, then you have to deal with it differently. I'm all for learning and reforming.