

The Financial Express

1. [Home](#)
2. [Opinion](#)
3. Deal with attack in Aadhaar right

Deal with attack in Aadhaar right

There can be little doubt UIDAI handled The Tribune expose badly by filing an FIR against the reporter who got access to personal information of people, albeit not their biometrics.

By: [Sunil Jain](#) | Published: January 9, 2018 5:13 AM



UIDAI later said it had no option since the law demands it report all events to the police. But why not acknowledge the role the journalist played and politely request her to help the authorities? (Source: IE)

TOP NEWS

There can be little doubt UIDAI handled The Tribune expose badly by filing an FIR against the reporter who got access to personal information of people, albeit not their biometrics. UIDAI later said it had no option since the law demands it report all events to the police. But why not acknowledge the role the journalist played and politely request her to help the authorities? Far more important is explaining why there wasn't unrestricted access to information. Since Aadhaar is a 12-digit random number, UIDAI can theoretically generate one lakh crore Aadhaars. With just 120 crore Aadhaar numbers, it is unlikely typing any 12-digit numbers would give the reporter access to a billion Aadhaar details; much less in 10 minutes; it would, in actuality, take years. As for getting the phone number/e-mail of a specific person, say [Aamir Khan](#), that would take forever given it is one of one lakh crore numbers. Chances are the journalist knew a few Aadhaar numbers of people and entered those to check whether the addresses/mobiles/email were correct. UIDAI missed a big opportunity to calm people's fears.

Frighteningly, for those who value privacy, there are easier ways to get Aamir Khan's numbers, even the value of his house. The Election Commission website allows you to download voter rolls for every area that also gives you the person's age and the name of the father/husband, apart from the address. It gets worse. Put in any surname in the municipal records, and you get the property ID of everyone in a colony with that surname. Enter that ID and, if the tax has been paid online, you can even know how much tax was

paid; even if it has not been paid online, you can get details like the phone number and email ID for the owner of each property.

But India Today too bought many personal details from an Aadhaar vendor. While that corroborates what Tribune found, if the same expose was to be done on a mobile phone or a PAN card vendor, chances are, you could get pretty much the same details. After all, the documents people submit as address/ID proof have these details. Where else do you think those pesky direct marketers get your details from? Most information got from various Aadhaar breaches can be got from many other places.

None of this means it is all right for Aadhaar vendors to leak your details, but UIDAI is trying to plug as many loopholes as it can.

Many government websites, in the interests of transparency, used to give details of the money paid for, say, your pension. The list would have your name, e-mail, phone number, address, and bank details. Last year, the Jharkhand government put out details of one million pensioners. Even if Aadhaar did not exist, these would have been put out. UIDAI and the electronics ministry have identified and stopped 200 websites from putting out such information, and told all departments that this is illegal.

While the media made much of the Maharashtra farm loan scam where thousands of farmers had the same Aadhaar and bank account numbers, the scam was discovered by UIDAI. When, in the Axis Bank case, the data-entry person was using stored biometric data instead of capturing fresh data each time, UIDAI discovered this and took action. Ditto for Kanpur where one of its operators had

made silicon copies of his fingerprints and was using these to get people to collect biometrics in different parts of the city simultaneously. The biometrics, by the way, were always secure since they are encrypted upon capture. And close to 250 fake apps that collected Aadhaar details were reported to [Google](#) for removal from the Play Store.

No system is foolproof, as the theft of money from bank accounts/credit cards makes clear. What is important, is that the organisation keeps ahead of the crooks, which is what UIDAI is doing. Apart from GPS on biometric-capture devices. At some point, even PoS machines can have this. And a rule that says only data coming from UIDAI-registered devices will be accepted, the PMLA rules were changed to ensure no bank account can be opened without Aadhaar authentication and that this exercise will have to be done for existing accounts as well. The latter will prevent rackets like the one in Hyderabad. Using information on names/addresses/Aadhaar numbers, fake bank accounts were created to transfer `40 lakh of government pensions.

Those attacking Aadhaar must keep in mind racketeers want it shut down/limited. Various central government benefits, the Economic Survey tell us, totalled `780,000 crore in FY17. Given around half never reached beneficiaries in the past, that's `390,000 crore reasons for racketeers to want to restrict Aadhaar. An Aadhaar-bank account-PAN link ensures no information is hidden from the taxman. And once Aadhaar is linked to every property, this will hit benaami ownership.

With so much at stake, the attacks on Aadhaar will multiply by giving leads/stories to journalists/activists who, to be fair, feel they are just doing their bit to protect privacy. All of which means UIDAI will have to really get its act together to investigate the exposes quickly, take necessary action fast- and explain what action has been taken- and explain why most of the stories are being overblown or interpreted incorrectly. It's not just public opinion, even the Supreme Court which is hearing petitions on Aadhaar needs to be assured the public's data is safe.