

Nobody can get any extra information about you once you link your mobile to your UID

The Phoney Aadhaar Bogey



RS Sharma

In November 2008, 10 members of Lashkar-e-Taiba carried out terrorist attacks across Mumbai, killing 164 persons. The attackers used at least three SIM (subscriber identification modules) cards purchased on the Indian side of the border with Bangladesh.

Would the terrorists have been deterred if they could not obtain disposable SIM cards on bogus ID papers? Probably not. But the security agencies may have had a sliver of hope in nabbing them and preventing the deaths.

In the dystopian view of alarmists, if we verify the subscriber's identity using his Aadhaar number, it would destroy the privacy of citizens. That is far from the truth. What is retained by the telecom company after acquiring or verifying the subscriber's ID is the record of authentication, not the biometric data itself. It is like a 'verified' tick-mark in the record.

A paper-based ID actually leaves additional information. For instance, a copy of a PAN (permanent account number) card also unnecessarily reveals the subscriber's PAN number. How's that better for protecting privacy?

Citizen Empowerment

A subscriber authenticated by Aadhaar gets quick activation of services and peace of mind that his identity cannot be used to issue connections to others, who may involve them in anti-social or criminal activities. For telecom compa-

nies, electronic KYC (know your customer) is cheaper and eliminates the risk that a rogue agent may cooperate in enrolling a subscriber with false identity. This problem must worry the telcos as fines to the tune of Rs 2,786 crore have been imposed on them on this account. The Telecom Regulatory Authority of India (Trai) has already stipulated that multiple authentications cannot be done in a short while to surreptitiously activate an extra SIM.

Consider, too, the problem that telcos face with paper-based Customer Acquisition Forms (CAFs). A sheet of A4 size paper weighs 5 gm. Assuming six sheets are required for enrolment, it means 30 gm per subscriber, or 30,000 tonnes of paper for a billion subscribers. That's 12 full-sized freight trains loaded with paper forms to store for 20 years. And the problem of locating one of those forms, when required. No wonder telcos are keen to go fully digital.

Once verified, the mobile becomes a secure digital ID that the subscriber can present to other entities, such as banks or government agencies providing e-services. It brings financial inclusion to those who hold a cellphone and a 12-digit number provided free by the government.

This combination also enables a frictionless payment system (powered by Unified Payment Interface, or UPI) that is rapidly getting embedded into products and services created not only by GoI but also by private businesses. The Jan-Dhan, Aadhaar and Mobile (JAM) trinity is a truly empowering tool, unique in the world.

The citizens seem happy to link their Aadhaar with the mobile, the telcos should be pleased with the advantages it offers, and GoI is helped in its effort to further national security, financial inclusion and provide a cheaper, more secure



FILE PHOTO

All your fears a phone link away... in your head

payment system.

All of this can, however, be no defence in breaching the law or a court order. Some activists have concluded that linking of Aadhaar with mobile numbers is against an order of the Supreme Court. This is untrue.

Spin-Offs For Many Sectors

The Supreme Court, concerned about the verification of subscribers' identities (Lokniti Foundation v. Union of India, 2017), asked GoI on its own to devise an effective method of reverification. It was in this context that GoI provided an undertaking to the court that it shall do an Aadhaar-based verification, which the court accepted. It also required that GoI complete the exercise within one year.

Authentication of identity does not breach privacy. If it did, nobody could ever be asked to present even a paper-based ID. Almost every country has some number to prove your ID – a social security number in the US, a national insurance number in Britain, etc.

The privacy concerns raised by alarmists are a bogey. Nobody gets any additional information about you because you were authenticated by the telecom company using Aadhaar.

GoI can, indeed, get assurance that the identity of the SIM owner

is verified. But you can't deny this assurance unless you advocate that SIMs should be issued anonymously. As of now, the status is that an anonymous SIM or one on forged ID is illegal.

That such SIMs can exist is a concern that agitated the Supreme Court and launched the reverification based on Aadhaar. Also, Trai gets a large number of references from the police where crimes have been committed and the mobile SIM owner cannot be traced.

With Aadhaar verification of users' identities, citizens are assured that the real owners of SIMs are known. This verification brings the only access to banking for some, and a very convenient one to the rest of us. It makes processes fraud-resistant, cheaper and faster, not only for the telcos, but for other sectors of economy too.

Aadhaar is the world's largest digital identity infrastructure, which is playing a transformational role in the economy and public policy of our country. Other countries are looking to learn from it. We ought not to permit misguided or motivated opposition to defeat India's interests.

The writer is Chairman, Trai, and was former CEO, Unique Identification Authority of India (UIDAI)

The privacy concerns raised by alarmists are a bogey. Nobody gets any additional information about you because you were authenticated by the teleco using Aadhaar.