Security questions

The Unique Identification Authority of India (UIDAI) has taken a firm step in support of data security and privacy by introducing disposable IDs, authentication tokens and tiered KYC requirements to reduce the exposure of Aadhaar numbers. These are logical measures, since providers only need to have the number authenticated against a person. There is no need for them to store it even for a second thereafter. This principle has been followed in other services for decades. For instance, email providers do not know their users' passwords, since they are not stored on servers in plain text. They are stored as hexadecimal hashes, which are cryptographically compared against passwords during a login. It is surprising that this pervasive principle, which is followed by almost all services requiring a login, was not applied to UIDAI earlier.

While the objectives of Aadhaar are entirely reasonable, its implementation has not earned universal trust. Apart from disastrous denials of the very services it was designed to assure — withdrawal of food and shelter entitlements to the poorest have been noted — the security of the world's biggest repository of biometric data has been questioned following leaks. The first problem is being examined by the courts. And the virtual ID is the UIDAI's first attempt to address the second. From the time the project was launched by Nandan Nilekani, its promoters chose to stonewall criticism, instead of engaging with it, by arguing that Aadhaar is an impregnable data silo. The UIDAI's reaction to a newspaper story which showed how easy it is to acquire Aadhaar numbers was to target the messenger. Just two months ago, the government claimed in an affidavit that Aadhaar is breach-proof.

There is an element of hubris here, and the technologists behind Aadhaar must know it. Systems are secured by multiple strategies, but there is no such thing as bulletproof security. All systems are vulnerable to a capable, imaginative and determined attacker, no matter how diligently they are secured. The only certain deterrent is legal, and fortunately privacy law has plugged the gap. However, it remains to be seen how many impugned parties have the stomach for private litigation. And the fact remains that large repositories of data, whether Equifax or Aadhaar, are targets in a world where data is the new gold. Their holdings must be shared on a need-to-know basis, and the recent blanket requirements for Aadhaar data to be shared with service providers, from mutual fund managers to telecom companies, flies in the face of that principle. Tiered exposure and virtual IDs would now reduce exposure of real Aadhaar numbers, though they must have already been shared in large quantities. Now, UIDAI has taken a step towards seeking universal trust, which is the bedrock of a legitimate authentication system.

END