ECONOMIC TIMES, Delhi, 26.1.2018

Page No. 18, Size:(12.87)cms X (27.12)cms.

Here Comes Step Two

V Sridhar & T K Srikanth

The UIDAI has responded with major revisions, in response to various criticisms on the security and privacy issues related to Aadhaar. The very first circular of the year from UIDAI Authentication Division on January 10 outlines the implementation of virtual ID (VID), unique identification (UID) token, and electronic Know Your Customer (eKYC) norms.

Of all problems cited, aggregation of information and secondary use of Aadhaar details are most prominent. Aggregation is the gathering together of information about a person.

A piece of information here or there is not very telling. However, when combined together, data begin to form a portrait of a person.

The Aadhaar number by itself does not tell anything. But when used to link various information such as mobile number, bank account, driver's licence and Permanent Account Number (PAN), the aggregated information can completely profile the individual. UIDAI has responded to this concern by creating the VID that is transient and not permanent.

The concept of the UID token generated is based on the VID of the user for each Authentication User Agency (AUA). The UID token is non-transient and is a function of the Aadhaar number, so that it can be used for de-duplication within the domain of the AUA. Say, if each bank is an AUA, de-duplication, if required, can be done within the same bank, but not across banks.

The UID token also removes the problem related to 'secondary use of information' — the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent. Since the UID token is valid only within the AUA, sharing it across AUAs is harmless. It can't be used for purposes other than what it is intended for.

The UIDAI needs to educate Aadhaar holders about the importance of VID, how and when to revoke and generate new ones.

The primary concern is regarding the onus and responsibility of AUAs that collect and submit Aadhaar numbers/VIDs to the Central Identities Data Repository (CIDR) for authentication. While the Aadhaar Act clearly specifies the responsibilities of AUAs, it is time that AUAs strictly adhere to the 'informed consent' principle. It's time that AUAs self-regulate themselves in the use and disclosure of personally identifiable information (PII) such as photographs, names and Aadhaar number/VID.

Though the UIDAI has a process for granting AUAs, and publishing the list of live AUAs on its website, the list should be easily accessible and searchable, perhaps through an Aadhaar mobile app, so that if individuals need to verify the authenticity of AUA, it can be done quickly. The UIDAI shall carefully scrutinise the requirements of Global AUAs (including government departments) before granting them access to a full KYC, including the Aadhaar number.

Aadhaar 2.0 is a good technical step to minimise the potential problems of privacy. The UIDAI circular also indicates that all AUAs need to comply with the technical requirements of revisions by June 1.

The proposed Data Protection Bill is expected to supplement the technical features with appropriate legislation.

However, we need to go one step further. As individuals, we need to be informed and exercise our rights while sharing information, evolve self-regulating AUAs, and adhere strictly to protecting the privacy of individuals.

The writers are professors, IIIT-Bangalore