

Through a Critical Lens-Unique Identification Authority of India

Khushboo

Aadhar--possibly the world's largest biometric identity system has been a contentious issue in India for many years now. Many believe that the system is helpful in weeding out ghost-identities and hence aids in the reduction of corruption and tax evasion and smoothen direct benefit transfer. However, concerns over data-protection and identity theft have been rising steadily with about 30 petitions having been filed since 2012 challenging various aspects of the Aadhar framework and the Aadhar (Targeted delivery of financial and other Subsidies benefits and services) Act 2016.



The government has recently made linking of bank accounts, mobile numbers and PAN cards to Aadhar a binding requirement. This has invited both positive and negative traction. The government argues that linking Aadhar to one's bank account will help eliminate fraud accounts and thus prevent benefit transfer to bogus

beneficiaries. It will also reduce tax leakages and money laundering. The Aadhar Enabled Payment System (AEPS) gives the user instant access to his or her account via micro ATM or a cell phone.

The problem with this, however, are manifold. Firstly, this implies that individuals not enrolled in the program are devoid of the benefit of social welfare schemes. Given that the Aadhar program is voluntary and not mandatory, as has also been emphasized by the Supreme Court, the very legitimacy of the idea comes under question.

Additionally, with the 'Right To Privacy' having been recognized as a fundamental right, upholding personal integrity has become an important part of the Aadhar debate. This further underscores the importance of the voluntary nature of the program as one must recognize the difference between willingly sharing personal information and being forced to do the same.

Further, it has been claimed that linking Aadhar to welfare schemes will help spread their benefit to the maximum number of people and potential beneficiaries will not remain devoid of these benefits due to lack of information. However, in stark contrast to this claim, it appears that these schemes are being used to popularise the Aadhar program by making enrolment a necessary condition for availing any scheme.

Furthermore, as defenders jump on the

linking of mobile numbers and bank accounts to Aadhar will help curb corruption by eliminating identity theft, Aadhar poses as much risk of creation of false identities through parting information to third-party organization as of prevention. While UIDAI claims that the data is encrypted with the security of the highest level, recent reports suggest otherwise.

Beyond the issues of privacy and surveillance, the use of biometrics as an identity for Aadhar is also contestable. Biometrics of an individual are subject to changes due to aging, manual labour or illness. The uniqueness of Aadhar hinges on the uniqueness of biometrics of an individual and hence updating biometrics need to be dealt with due importance in the framework. However, the Aadhar Act does not lay any pointed emphasis on the same. Thus, Aadhar is highly susceptible to identity theft. If one fakes the biometric authentication, Aadhar enabled identity theft can be committed as the security of the database itself is not a factor to consider at all.

The issues surrounding Aadhar pose a much deeper question of an inadequate legal framework for personal data protection in India. The Aadhar Act cannot assume the role of a comprehensive law on personal data; technology-centric data protection norms need to be established before increasing the ambit of the Aadhar program any further. The problem of a weak legal structure on data protection is further exacerbated by the fact that India houses a user base with high digital illiteracy, which without protection makes them a likely target for exploitation by third party service providers.

Recent changes adopted by the UIDAI include incorporating face identification along with fingerprint scanning and

creation of a tokenized security system that claims to make linking of Aadhar a strictly one-way process. These changes while welcome also come across as an admission of fallacies in the system by UIDAI and further validate apprehensions surrounding the program. The fact that UIDAI is finding it difficult to defend the Aadhar framework is blatantly apparent. Its unwillingness to engage with stakeholders and lack of clarity about data security norms further accentuate the problem and weaken its position.

Although rubbished as ‘paranoia’ by defenders of the ambitious project, the fear of creation of a surveillance state is not without reason.