Vulnerabilities in the UIDAI Implementation

NOT ADDRESSED BY THE AADHAAR BILL 2016

APPLICATION
to Enrollment Agencies (EAs)

ELIGIBILITY
through a proof of identity or the Introducer system

Introducer system is not foolproof, leads to **lack of accuracy and national security concerns**

CONSENT

Lack of specifications on what the consent form should state **could lead to blanket consent and little control on data**

DATA COLLECTION

Some Registrars permitted to collect more information and **extra/unnecessary information collected in the guise of UID enrollment**

BIOMETRICS COLLECTION

Collection through vendor-supplied devices which give **access to third parties, including those not governed by Indian law**

BIOMETRICS EXCEPTION
applicable if the individual's eyes/hands are amputated/missing

This clause has been used by the EAs for **fraudulent entries to inflate number of enrollments**

VERIFICATION

Identity fraud & national security concerns because verification process is not robust enough

BANK ACCOUNT OPENING AUTHORIZATION

Correction/retraction of data difficult
Could lead to **exclusion from benefits** of those opting out

DATA ENTRY
manually entered by operators into UIDAI provided software

Data operators answerable to EA, not to UIDAI leading to **risk of misuse/ loss of data**

STORAGE AND BACKUP
by Enrollment Agencies (EAs)

backup maintained for 60 days minimum

This **creates data security risk, and national security risks** as some vendors *may* have links with foreign intelligence agencies.

DATA DE-DUPLICATION
by Central Identities Data Repositor (CIDR)

on receiving biometric information, de-duplication is done to ensure that each individual is given only one UID number

High rate of rejection of Aadhaar applications and independent review of technology **raises questions about efficacy of de-duplication technology, and concerns remain about manual checking**

THE CENTRE FOR internet & society